P05 – Relatório de Segurança do Sistema de Bilhetagem Eletrônica

(DC2) Uso Restrito na PwC - Confidencial

Projeto de Auditoria e Consultoria para Revisão, Definição e Implantação de Modelo de Auditoria e Fiscalização dos Contratos e Avaliação Estratégica do Sistema de Ônibus

Dezembro de 2014

Etapa 2 - Auditoria do Sistema de Bilhetagem Eletrônica (SBE)

P05 – Relatório da Segurança do Sistema de Bilhetagem Eletrônica

Rio de Janeiro, 3 de dezembro de 2014.

À
Secretaria Municipal de Transporte
Prefeitura da Cidade do Rio de Janeiro

Atenção: V. Exª. Sr. Alexandre Sansão Fontes
Secretário Municipal de Transportes do Rio de Janeiro

Prezado Senhor:

De acordo com Termo de Referência referente à Etapa 2 do Projeto de Projeto de Auditoria e Consultoria para Revisão, Definição e Implantação de Modelo de Auditoria e Fiscalização dos Contratos e Avaliação Estratégica do Sistema de Ônibus, apresentamos a seguir nosso Relatório da Segurança do Sistema de Bilhetagem Eletrônica (SBE).

Nossos trabalhos consistiram na realização de uma série de testes no ambiente tecnológico da RioCard, responsável pelo processo de bilhetagem eletrônica do Município do Estado do Rio de Janeiro durante o período de 04 de agosto à 30 de novembro de 2104. Como resultado, elaboramos um relatório detalhado contendo a abordagem adotada, resultados obtidos e recomendações sugeridas; não abrangendo, portanto, procedimentos orientados aos exames das demonstrações financeiras, de responsabilidade dos auditores externos. Assim, não estaremos em condições de emitir, e não emitiremos, parecer sobre as suas demonstrações financeiras e sobre os processos objetos de nossa revisão.

A PwC não assume qualquer responsabilidade para com terceiros em relação aos resultados aqui reportados.

Ressaltamos que nossos trabalhos não esgotam futuras análises ou revisões específicas e mais amplas que poderão, eventualmente, identificar outros aspectos de melhoria.

Permanecemos à disposição para quaisquer esclarecimentos.

Atenciosamente,

Ronaldo Matos Valiño
PRICEWATERHOUSECOOPERS

Conteúdo

1. Introdução 5

2. Abordagem e Etapas do Projeto 9

3. Resultados Obtidos 13

3.1. Deficiências/Divergências Identificadas Relacionadas aos Aspectos de Segurança da Informação e Recomendações Sugeridas 13

3.1.1. Organização da Segurança da Informação 13

3.1.1.1. Análise da Documentação de Segurança da Informação 13

3.1.2. Avaliação da Segurança dos Cartões 16

3.1.2.1. Análise de documentação e processo de geração de chaves de segurança 16

3.1.2.2. Análise de documentação e processo de fabricação e validação dos cartões 19

3.1.3. Segurança física e do ambiente 22

3.1.4. Gerenciamento das operações e comunicações 24

3.1.5. Controle de acesso lógico 28

3.1.6. Gestão de incidentes de segurança da informação 32

3.1.7. Aquisição, desenvolvimento e manutenção de sistema de informação. 33

3.1.8. Gestão da continuidade do negócio 35

3.1.9. Avaliação dos ambientes e meios físicos onde os diversos componentes do SBE estão dispostos 38

3.1.10. Avaliação das redes de comunicação 39

4. Testes de Intrusão 42

4.1. Teste externo de intrusão em aplicação web e infraestrutura 42

4.1.1. Abordagem e escopo do Projeto para o teste de intrusão externo 42

4.1.2. Resultados Obtidos 45

4.1.3. Análise e Validação das vulnerabilidades 59

4.1.3.1. Teste de invasão externo de aplicação web 59

4.1.3.2. Teste de invasão externo de infraestrutura 87

4.2. Teste externo de intrusão em ambiente interno 92

4.2.1. Testes realizados e resultados obtidos 93

Anexo A – Fluxograma do processo de geração das chaves 101

Anexo B – Fluxograma do processo de fabricação de cartões 102

Anexo C – Matriz de Vulnerabilidades de Aplicação Web 103

Anexo D – Matriz de Vulnerabilidades de Infraestrutura 112

Anexo E – Lista de verificações realizadas pela ferramenta automatizada 115

Anexo F - Glossário 122

1. Introdução

Este relatório é parte integrante da **Etapa 2** do projeto de **Auditoria e Consultoria para Revisão, Definição e Implantação de Modelo de Auditoria e Fiscalização dos Contratos e Avaliação Estratégica do Sistema de Ônibus**, que contempla três produtos (relatórios) em sua totalidade, sendo eles:

- ✓ P04 - Relatório de Avaliação das Regras de Negócio;
- ✓ P05 - Relatório da Segurança do Sistema de Bilhetagem Eletrônica (SBE); e
- ✓ P06 - Relatório de Funcionalidades.

O relatório em questão (P05) possui como objetivo avaliar a segurança relacionada ao ambiente tecnológico em que o Sistema de Bilhetagem Eletrônica (SBE) encontra-se em operação, considerando os processos, infraestrutura, interfaces, comunicação de dados e sistemas de tecnologia da informação e comunicação.

Desta forma, conforme definido no referido Termo de Referência, as seguintes atividades fizeram parte do escopo de nosso trabalho:

1. ***Organização da segurança da informação existente***, incluindo: estrutura, políticas, normas e procedimentos;

2. ***Segurança física e do ambiente***, em especial os controles de entrada e saída física, proteção contra ameaças externas e do meio ambiente e segurança de equipamentos;

3. ***Gerenciamento das operações e comunicações***: procedimentos e responsabilidades operacionais, documentações dos procedimentos de operação, gestão de mudanças, segregação de funções, separação dos recursos de desenvolvimento, teste e de produção, gerenciamento de serviços terceirizados, cópias de segurança, gerenciamento da segurança em rede e políticas / procedimentos para troca de informações e monitoramento;

4. ***Controle de acesso lógico de todos os sistemas envolvidos***: requisitos de negócio para controle de acesso, gerenciamento controle de acesso às redes de dados envolvidas; política de uso dos serviços de rede; autenticação para conexão externa do usuário; proteção e configuração de portas de diagnóstico remotas; segregação de redes; controle de conexão de rede; controle de roteamento de redes; procedimentos seguros de entrada no sistema

(log-on); identificação e autenticação de usuário; sistema de gerenciamento de senha; desconexão de terminal por inatividade; controle de acesso à aplicação e à informação; restrição de acesso à informação;

5. ***Gestão de incidentes de segurança da informação***: fornecer o atendimento tempestivo aos chamados de incidentes de segurança da informação, através de uma solução de contorno ou reparo rápido e, dessa forma, minimizar o impacto no negócio ocasionado pela indisponibilidade do serviço afetado.

6. ***Aquisição, desenvolvimento e manutenção de sistemas de informação***, abrangendo SLAs (Acordo de Níveis de Serviço) e ciclo de desenvolvimento de software seguro (utilização de técnicas para proteger a aplicação de vulnerabilidades durante o desenvolvimento);

7. ***Gestão da continuidade do negócio***: aspectos relativos à segurança da informação (procedimentos para proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil); e continuidade de negócios e análise/avaliação de riscos (se a gestão da continuidade do negócio inclui controles para identificar e reduzir riscos, em complementação ao processo de análise/avaliação de riscos global, limitando as consequências aos danos de incidentes e garantindo que as informações requeridas para os processos do negócio estejam prontamente disponíveis);

8. ***Testes de intrusão em infraestrutura e aplicações envolvidas, com base em abordagem whitebox*[1] *(.*** Para a realização desses testes utilizamos metodologia própria da PwC baseada na norma ISO 15408, OWASP (Open Web Application Security Project) e na experiência dos nossos profissionais. Adicionalmente, consideramos a execução de testes previstos na Classe AVA (*Vulnerability Assessment*) da ISSO 15408, incluindo os seguintes testes:

✓ *SQL Injection*
✓ *Code Injection*
✓ Manipulação de URLs
✓ Validação de dados
✓ Escalação privilégios
✓ Obtenção de informações – *sniffer*
✓ *Cross-site Scripting (XSS)*
✓ Inclusão de arquivos
✓ Manipulação de Cookies
✓ Manipulação de campos de dados
✓ Utilização de informações em mensagens de erro
✓ Uso de sessão de terceiros
✓ Quebra de criptografia
✓ *Vulnerabilidades de AJAX (Asynchronous JavaScript and XML)*

9. ***Avaliar os ambientes e meios fisicos onde os diversos componentes do SBE estão dispostos***, localizados na RioCard;

10. ***Avaliar as redes de comunicação quanto à integridade, disponibilidade e confidencialidade, entre os ambientes e meios físicos***, localizados na RioCard;

11. ***Avaliar a segurança dos cartões utilizados nos validadores***, em especial quanto à qualidade das chaves de segurança utilizadas e à possibilidade de sua violação;

---

[1] **Análise whitebox:** Tipo de análise de teste de invasão que consiste na obtenção de detalhes da aplicação (e sua infraestrutura de suporte) são fornecidos ao inicio dos trabalhos. Este tipo de abordagem assume o pior cenário possível, onde um atacante já obteve as informações sobre o sistema observado e possui as credenciais necessárias para realizar uma análise completa da aplicação e/ou seus controles de segurança da infraestrutura. Ao se apresentar essa abordagem o cenário exclui o tempo necessário (e disponível a um atacante) para se obter os conhecimentos para realizar tal tipo de ataque. Isso torna possível ao contratante obter uma visão total de todos os ângulos de ataque disponíveis a alguém com o tempo hábil para a realização do ataque. Dentro dessa abordagem todos os tipos de ataque que trazem um potencial risco ao contratante são discutidos antes do efetivo teste, assim nenhuma ação de maior risco é tomada sem o conhecimento e aprovação do contratante.

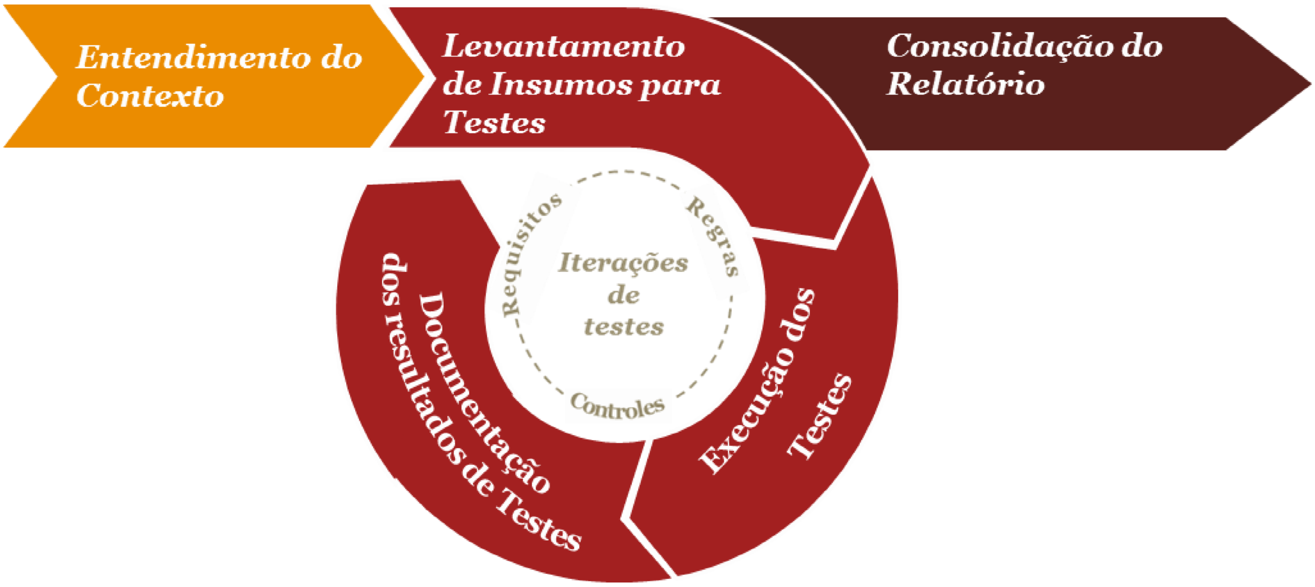
Para atender as atividades previstas anteriormente utilizamos como referência os modelos de qualidade preconizados no mercado relacionado à tecnologia da informação:

ISO 9000-3 ®; NBR ISO/IEC 27001 ®; NBR ISO/IEC 27002 ®; ISO/IEC 15408 ®; ISO/IEC 15504 ®; NBR ISO/IEC 25051 – Engenharia de Software - Requisitos e avaliação da qualidade de produto de software; NBR ISO/IEC 14598 – Tecnologia de informação – Avaliação de produto de software – Parte 5. OWASP ®; e CobIT 5 ®.

2. Abordagem e Etapas do Projeto

Para atender os objetivos definidos para esse relatório, adotamos a abordagem segregada nas etapas abaixo e demonstradas na Figura 1:

Figura 1 – Etapas do Projeto


Entendimento do Contexto
Levantamento de Insumos para Testes
Consolidação do Relatório
Execução dos Testes
Documentação dos resultados de Testes
Iterações de testes
Requisitos
Regras
Controles

I. Entendimento do Contexto

Nesta etapa foram realizados o levantamento e o entendimento a respeito das políticas, padrões e procedimentos com objetivo de obter uma compreensão a respeito das legislações, políticas, padrões, procedimentos, e ambiente tecnológico do Sistema de Bilhetagem Eletrônica (SBE). Desta forma, executamos as seguintes atividades:

(a) Preparação de documentação de solicitação de informações;

(b) Envio de documento de preparação de roteiro de entrevistas, bem como definição de datas de entrevistas a serem realizadas com os gestores responsáveis;

(c) Obtenção de documentação preliminar com base em resultado das entrevistas realizadas; e

(d) Análise da documentação recebida.

II. *Levantamento de insumos para testes*

Nesta etapa foram realizadas entrevistas de aprofundamento de entendimento a respeito de cada um dos itens avaliados. Para isto, as seguintes atividades foram executadas:

(a) Acompanhamento das atividades e controles realizados (processo de *walkthrough*);

(b) Documentação do entendimento do processo realizado no item (a) acima;

(c) Mapeamento de riscos e controles existentes em cada processo avaliado. Nessa atividade consideramos como base os modelos existentes no mercado e descritos na seção anterior que foram base para nossa análise;

(d) Definição das necessidades de informações para realização dos testes (necessidades de evidências);

(e) Elaboração dos Planos de Testes; e

(f) Envio da solicitação de informações para realização dos testes.

III. *Execução dos testes*

Nesta etapa foram executados os Planos de Testes, definidos e documentados na Etapa anterior, com o objetivo de confirmar a aderência dos controles identificados e mitigação dos riscos associados. Para isto, as seguintes atividades foram executadas:

(a) Execução dos planos de testes, considerando as seguintes abordagens:

- **Extensão dos testes**

Os testes foram realizados com base na metodologia de auditoria da PwC (PwC Audit Guide) que é estruturada de acordo com as melhores práticas de auditoria.

Para os testes de controles manuais, utilizamos uma base amostral a partir do universo de ocorrências relacionadas ao controle conforme previsto no capítulo “PwC AG 6053 - Extensão dos testes” presente na metodologia PwC, onde utilizamos o quadro de seleção de itens abaixo com base na frequência do controle (*vide tabela 1*).

Tabela 1 – Quadro de Seleção de itens para testes de controles manuais

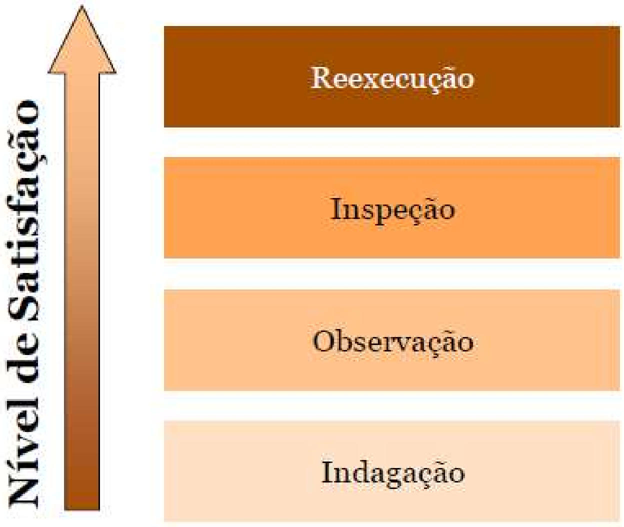
Frequência do Controle	População assumida (ocorrências de controle em todo o ano)	Números de ítens para teste
Anual	1	1
Trimestral	4	2
Mensal	12	2
Semanal	52	5
Diário	250	20
Múltiplas vezes ao dia	Acima de 250	25

Para testes de controles automatizados, obtivemos uma ocorrência por cenário de controle a ser testado conforme capítulo “PwC AG 6054 – Testando Controles Automatizados”.

– Natureza dos testes

A natureza dos testes considerou um agrupamento de pelo menos duas naturezas de testes, conforme figura 2 abaixo, baseado na metodologia da PwC (PwC *Audit Guide* 6052 – Natureza dos testes de Controle).

Figura 2 – Natureza dos testes de controles



- **Período do teste**

  O período dos nossos testes compreenderam o período de 01.01.2014 até a data da realização do referido teste, que foram realizados ao longo do 2º semestre de 2014.

(b) Documentação dos resultados obtidos

IV. Documentação dos resultados dos testes

Nesta etapa foram realizadas as análises dos resultados dos testes, bem como a elaboração de recomendações nos casos de identificação de deficiências de controle. Para isto, executamos as seguintes atividades:

(a) Análise dos resultados dos testes;

(b) Consolidação da documentação de resultados dos testes;

(c) Confirmação dos resultados dos testes; e

(d) Elaboração de recomendações de melhorias.

V. Consolidação do Relatório

Após a execução de todas as análises previstas para cada frente de trabalho, consolidamos os produtos finais previstos pelo projeto. Para isto, executamos as seguintes atividades:

(a) Consolidação das avaliações de cada frente de trabalho;

(b) Apresentação dos resultados através da execução de *workshops* técnicos de validação dos resultados;

(c) Elaboração do Relatório;

(d) Apresentação dos resultados finais; e

(e) Obtenção do aceite formal quanto às entregas realizadas.

3. Resultados Obtidos

3.1. Deficiências/Divergências Identificadas Relacionadas aos Aspectos de Segurança da Informação e Recomendações Sugeridas

Nesta seção detalhamos as deficiências, divergências e distorções relacionadas aos aspectos de Segurança da Informação, e as recomendações sugeridas para tratamento das mesmas. Os tópicos 3.1.1. e 3.1.2 deste relatório foram realizados com base na análise da documentação disponibilizada. Para os demais tópicos detalhamos os riscos e os objetivos de controle relacionados a cada um dos processos avaliados.

3.1.1. Organização da Segurança da Informação

3.1.1.1. Análise da Documentação de Segurança da Informação

Procedimentos executados

Realizamos reunião em 29.10.2014 para obter entendimento em relação à estrutura estabelecida na área de Segurança e Conformidade da RioCard. Adicionalmente, obtivemos algumas informações / documentação para análise, sendo: organograma, políticas, normas e procedimentos aplicados na referida área.

Estrutura e Responsabilidades

Resultados obtidos

Identificamos que o objetivo e responsabilidades atribuídas à Gerência de Segurança e Conformidade não estão alinhados com seus papéis e responsabilidades.

Como exemplo, citamos a área de Central de Serviços, que possui como objetivo atendimento às demandas de usuários, e encontra-se sob gestão da própria gerência de Segurança e Conformidade.

Adicionalmente, a Gerência de Segurança possui também como responsabilidade executar o mapeamento de processos e verificar sua conformidade, acarretando na ausência de segregação de funções.

Recomendações

Rever os papéis e responsabilidades da Gerência de Segurança e Conformidade adequando sua estrutura às necessidades do negócio e redirecionando determinadas atividades.

Política

Resultados obtidos

Identificamos a existência de uma política de segurança da informação atualizada em 10/04/2013.

Recomendações

A Política de Segurança da Informação deverá ser revisada tempestivamente dentro de períodos regulares, definidos pelas gerências de mudanças e de configurações, e anualmente, conforme estabelecido na própria Política de Segurança da Informação (item 8. Controle e Manutenção) para garantir que esteja alinhada aos objetivos estratégicos e forneça as diretrizes corretas.

Normas

Resultados obtidos

Identificamos a existência das seguintes normas: (a) Controle de Acesso; (b) Gestão de Pessoas; (c) Gestão de Ativos; (d) Operações e Comunicações; (e) Gestão, aquisição e desenvolvimento seguro de sistemas; (f) Utilização de correio eletrônico; (g) Gestão de trilhas de auditoria; (h) Gestão de incidentes de segurança da informação; (i) Gestão de segurança física e ambiental.

Entretanto, as seguintes normas não obtiveram uma revisão tempestiva (maiores que 1 (um) ano de revisão/atualização), com posterior atualização: (a) Gestão de Pessoas (última atualização em 20.05.2013) e (b) Gestão de Ativos (última atualização em 20.05.2013).

Outras normas encontram-se com atualização inferior à 1 (um) ano e requerem atenção futura, sendo elas: (a) Operações e Comunicação (última atualização em 17.10.2013); (b) Gestão, aquisição e desenvolvimento seguro de sistema (última atualização em 17.10.2013); (c) Utilização de correio eletrônico (última atualização em 08.10.2013); e (d) Gestão de trilha de auditoria (última atualização 11.12.2013).

Recomendações

As normas deverão ser revisadas tempestivamente dentro de períodos regulares, definidos pelas gerências de mudanças e de configurações, e anualmente, conforme estabelecido na Política de Segurança da Informação (item 8. Controle e Manutenção) para garantir que estejam atualizadas conforme as necessidades de negócio.

Procedimentos

Resultados obtidos

Não identificamos procedimentos descritos para a área de Segurança e Compliance.

Recomendações

Sugerimos que sejam criados procedimentos com base nas normas e que estas apareçam referenciadas nos procedimentos para que desta forma seja possível compreender a diretriz que norteou o procedimento.

Adicionalmente, sugerimos a revisão destes procedimentos dentro de períodos regulares, definidos pelas gerências de mudanças e de configurações, e anualmente para que estejam em linha com a Política de Segurança da Informação.

3.1.2. *Avaliação da Segurança dos Cartões*

3.1.2.1. Análise de documentação e processo de geração de chaves de segurança

Procedimentos executados

Realizamos reunião em 25/09/2014 para obter o entendimento em relação às chaves de segurança utilizadas na RioCard e a possibilidade de sua violação.

Adicionalmente, obtivemos o fluxograma do cerimonial das chaves *(vide Anexo A)*.

Definição das chaves

Resultados obtidos

As chaves utilizadas pela RioCard são criptografadas com SSL de 2048 bits.

Recomendações

Entendemos que o nível de criptografia das chaves é adequado, não existindo necessidade de recomendação específica para esse item.

Armazenamento e manipulação

Resultados obtidos

Para armazenar as chaves privadas é utilizado um repositório central, cujo acesso só é permitido ao gestor da área de Segurança e Conformidade. Toda a gestão e contenção das chaves dos *smartcards* é feita por intermédio do HSM (*Hardware Security Module*) através de funções pré-definidas invocadas pelo código-fonte dos sistemas da RioCard pelo ICSF (IBM *Cryptography System Facility*), um *hardware* dedicado a funções de criptografia, servindo assim como acelerador criptográfico e também como cofre para as chaves.

Para garantir a não violação delas, é feito um processo de *hardening*[2]. Se este for comprometido, as chaves deverão ser geradas novamente.

Recomendações

Entendemos que o procedimento e softwares utilizados são adequados, não existindo necessidade de recomendação específica para esse item.

Permissões de Acesso

Resultados obtidos

Para executar as funções de criptografia, são necessárias permissões de usuário, que são constantemente monitoradas. O único usuário que tem permissão de editá-las é o CSIMP, cujo acesso é revogado e monitorado, com alertas específicos para verificar sua inativação.

As permissões que podem ser alteradas são exclusivamente referentes ao uso das funcionalidades da ferramenta, e não de acesso às chaves.

Recomendações

Entendemos que o processo está adequado, não existindo necessidade de recomendação específica para esse item.

---

[2] *Hardening* - Proteção e monitoração dos servidores

[2] *Seed* –Palavra-chave utilizada como referência para o cálculo da criptografia

Cerimonial

Resultados obtidos

A RioCard possui um método de contingência para a inutilização da chave-mestra do sistema. Esse método consiste na geração de uma nova chave idêntica à anterior, com o objetivo de manter a compatibilidade com os registros criptografados com a chave anterior, através da obtenção da *seed*[3] que está dividida entre 3 (três) diretores, cada uma com 2 (dois) fragmentos.

Não é realizado *backup* das chaves, pois o acesso direto a elas não é permitido.

O procedimento de obtenção da *seed* (chamado de "Cerimonial de Chaves") será necessário em caso de falha catastrófica ou *upgrade* no *mainframe* onde se faça necessária sua substituição, ou para ativação do ambiente de contingência em São Paulo.

Recomendações

Entendemos que o processo está adequado, não existindo necessidade de recomendação específica para esse item.

Unicidade dos Cartões

Resultados obtidos

Para coibir a prática de clonagem de cartões, a RioCard monitora o contador de transações dos cartões, que é incrementado a cada vez que ele é utilizado. Se houverem duas transações com o mesmo contador e mesmo número do cartão, todos os cartões com aquele ID são bloqueados.

Recomendações

Adicionalmente ao controle implementado, sugerimos que seja criado e implementado um controle no Sistema de Bilhetagem Eletrônica (SBE) que verifique se o cartão relacionado à transação consta como ativo na base de cartões válidos.

3.1.2.2. *Análise de documentação e processo de fabricação e validação dos cartões*

Procedimentos executados

Realizamos reunião em 02.10.2014 para obtenção do entendimento em relação à fabricação e validação dos cartões utilizados no Sistema de Bilhetagem Eletrônica (SBE) que são emitidos pela RioCard.

Solicitação de produção de cartões

Resultados obtidos

A produção de cartões RioCard pode ser solicitada por 3 (três) frentes: (a) área de Planejamento de Produção da RioCard; (b) área de Gerência de Gratuidade; e (c) através dos pedidos de clientes (usuários) através do site "Compradores VT", que podem ser empresas concedendo vale-transporte aos seus funcionários ou pessoas físicas administrando o próprio cartão e de seus familiares *(vide Anexo B para o fluxograma de produção de cartões)*.

Recomendações

Entendemos que o processo está adequado, não existindo necessidade de recomendação específica para esse item.

Gestão do Estoque

Resultados obtidos

A área de Estoque recebe o encaminhamento do pedido da área de produção e realiza uma consulta de disponibilidade dos materiais. Se não houver recursos disponíveis, são adquiridos mais cartões do fornecedor ou obtidos cartões recuperados na reciclagem.

Recomendações

Entendemos que o processo está adequado, não existindo necessidade de recomendação específica para esse item.

Inicialização dos Cartões

Resultados obtidos

A área de Produção prepara o cartão para ser utilizado no Sistema de Bilhetagem Eletrônica (SBE), substituindo-se a chave padrão do fornecedor por uma proprietária da RioCard. Também é realizada a personalização e carga dos cartões conforme o pedido.

Recomendações

Entendemos que o processo está adequado, não existindo necessidade de recomendação específica para esse item.

Reciclagem

Resultados obtidos

Os cartões do tipo Vale-Transporte Rápido são comprados pela Riocard e passam por um processo de triagem, onde são verificados quais poderão ser reutilizados, conforme processo de reciclagem (limpeza, empacotamento e, devolução ao estoque).

Os cartões do tipo Bilhete Único Carioca Pré-Pago podem ser adquiridos nos guichês do BRT gratuitamente mediante a uma recarga de, no mínimo, o valor da passagem modal (R$3,00 atualmente). Estes cartões podem ser reutilizados/recarregados ou devolvidos espontaneamente pelos próprios usuários.

Recomendações

Sugerimos a ampliação da campanha de recarga/devolução dos cartões Bilhete Único Carioca Pré-Pago, evitando desperdício e aumentando a sustentabilidade do programa.

Produção

Resultados obtidos

Os cartões retirados do estoque para atender uma solicitação são conferidos e, em caso de rejeição, são verificados quanto ao motivo do problema, podendo reabastecer o estoque ou ser descartados. Os que não apresentam problemas são enviados para expedição.

Recomendações

Entendemos que o processo está adequado, não existindo necessidade de recomendação específica para esse item.

Entrega

Resultados obtidos

A área de Expedição recebe os cartões e verifica os pedidos, encaminhando-os para o recipiente, que pode ser a Gerência de Gratuidade, Lojas RioCard ou domicílio do comprador. Para as Lojas RioCard, a forma de postagem é malote.

Para as residências, o método de envio é pelos Correios.

Recomendações

Sugerimos a realização da conferência de documentos pessoais para realização de desbloqueio do cartão, a fim de evitar o uso do cartão por terceiros em caso de extravio de correspondência.

3.1.3. *Segurança física e do ambiente*

I.1. – Gerenciar o Ambiente Físico – Item 2.3.2 do Termo de Referência

Processo responsável por garantir a segurança física e do ambiente, em especial os controles de entrada e saída física, proteção contra ameaças externas e do meio ambiente e segurança de equipamentos.

ID	Riscos	Objetivos de Controle	Resultado Obtido	Oportunidades de Melhoria
1	Não identificação tempestiva das ameaças à segurança física do Datacenter.	Assegurar o monitoramento contínuo que possibilite o tratamento tempestivo de ameaças relacionadas à segurança do Datacenter.	Não há documentação formal, mapeando e avaliando os possíveis impactos no ambiente de TI (DataCenter). Não há manuais operacionais padrão, para resposta aos alarmes ambientais.	Mapear e avaliar os impactos de desastres nas instalações de TI (Datacenter). Definir manuais operacionais para resposta a alarmes ambientais.
2	Não identificação tempestiva das ameaças à segurança física do Datacenter.	Assegurar que para todo alerta de incidente relacionado ao ambiente do Datacenter seja tempestivamente tratado.	Não identificamos até a data de 22/09/2014 a evidência de formalização da conclusão do tratamento pelo GOPER[4], do incidente "Máquina de Ar condicionado AC03 do datacenter parada", originado pelo alerta disparado pelo NetBotz em 12/08/14. às 02:17AM.	Manter o registro dos incidentes nas instalações, alinhados com o processo de gerenciamento de incidentes.

---

[4] GOPER – Gerência de Operações

I.1. – Gerenciar o Ambiente Físico – Item 2.3.2 do Termo de Referência

Processo responsável por garantir a segurança física e do ambiente, em especial os controles de entrada e saída física, proteção contra ameaças externas e do meio ambiente e segurança de equipamentos.

ID	Riscos	Objetivos de Controle	Resultado Obtido	Oportunidades de Melhoria
3	Danos à infraestrutura de TI causados por ameaças ambientais[5].	Assegurar que o Datacenter esteja equipado com equipamentos que protejam os servidores contra ameaças ambientais.	Controle Efetivo	Não aplicável

---

[5] Uma ameaça ambiental é um evento ou fenômeno que pode afetar potencialmente a vida, a propriedade e a atividade humana, devido a condições ou processos biológicos, geológicos, sísmicos, hidrológicos ou meteorológicos.

3.1.4. *Gerenciamento das operações e comunicações*

II.1. – Executar Procedimentos Operacionais – Item 2.3.3 do Termo de Referência

Processo responsável pelo gerenciamento das operações e comunicações, em especial os procedimentos e responsabilidades operacionais, documentações dos procedimentos de operação, gestão de mudanças, segregação de funções, separação dos recursos de desenvolvimento, teste e de produção, gerenciamento de serviços terceirizados, cópias de segurança, gerenciamento da segurança em rede e políticas/procedimentos para troca de informações e monitoramento.

ID	Riscos	Objetivos de Controle	Resultado Obtido	Oportunidades de Melhoria
1	Não detecção de indisponibilidade de recursos	Assegurar o monitoramento contínuo que possibilite o tratamento tempestivo de anomalias na utilização dos recursos computacionais do ambiente de produção.	Não existem documentações formalizadas que definem critérios sobre quais falhas devem gerar incidentes; Não existem planos de ação documentados para tratamento dos incidentes;	Elaborar documentação formal que definem os critérios sobre quais falhas devem gerar incidentes; Definir procedimentos para acompanhamento de todos os incidentes na Central de serviços; Referenciar os chamados de incidentes abertos junto à falha (origem do incidente) na ferramenta Nagios; Elaborar Planos de ação para os incidentes mais frequentes;
2	Falhas de Segurança	Assegurar o monitoramento contínuo que possibilite o tratamento tempestivo de ameaças relacionadas à segurança do ambiente de rede.	Não existem documentações formalizadas que definem critérios sobre quais alertas devem gerar incidentes; Não existem planos de ação documentados para tratamento dos incidentes.	Elaborar documentação formal que definem os critérios sobre quais alertas devem gerar incidentes; Definir procedimentos para acompanhamento de todos os incidentes na Central de serviços;

II.2. – Gerenciar Mudanças – Item 2.3.3 do Termo de Referência

Gerenciar todas as alterações de forma controlada, incluindo mudanças padrão e manutenção emergencial relacionada a processos de negócio, aplicações e infraestrutura. Isto inclui os padrões de mudança e procedimentos, avaliação de impacto, priorização e autorização, mudanças emergenciais, monitoramento, registro, encerramento e documentação.

ID	Riscos	Objetivos de Controle	Resultado Obtido	Oportunidades de Melhoria
1	Mudanças realizadas no ambiente de TI afetarem a disponibilidade e o desempenho do sistema SBE.	Garantir que as mudanças no ambiente de TI sejam avaliadas quanto ao risco e impacto no negócio, por profissionais competentes, com base em critérios pré-definidos, e com base nisso, devidamente planejadas através de projetos e planos de ação e remediação.	Não há políticas e procedimento formalizados que determine as práticas adequadas para o processo de avaliação de impacto e risco de mudanças.	Estabelecer práticas de Gestão de Mudanças, definindo aspectos como: Avaliação dos riscos envolvidos.
2	Mudanças não autorizadas serem realizadas no ambiente de TI.	Garantir que apenas as mudanças no ambiente de TI formalmente aprovadas pelos responsáveis competentes sejam executadas.	Não há políticas e procedimento formalizados que determine as práticas adequadas para a aprovação formal de mudanças.	Estabelecer uma Norma de Gestão de Mudanças, definindo aspectos como a Governança (papéis e responsabilidades) sobre as mudanças.
3	Acesso não autorizado ao ambiente de TI.	Garantir que as concessões de acesso com privilégios, concedidas para mudanças no ambiente de TI, sejam adequadamente controladas e tempestivamente revogadas.	Não há políticas e procedimento formalizados que determinem as práticas adequadas para a autorização, monitoramento e revogação de acessos temporários de *superusuários*, para tratamento de mudanças.	Formalizar uma Norma de Gestão de Mudanças, definindo, dentre outros, aspectos como: – tratamento de mudanças emergenciais; – governança sobre as mudanças; e – implementação de processo de monitoramento contínuo das mudanças.

II.2. – Gerenciar Mudanças – Item 2.3.3 do Termo de Referência

Gerenciar todas as alterações de forma controlada, incluindo mudanças padrão e manutenção emergencial relacionada a processos de negócio, aplicações e infraestrutura. Isto inclui os padrões de mudança e procedimentos, avaliação de impacto, priorização e autorização, mudanças emergenciais, monitoramento, registro, encerramento e documentação.

ID	Riscos	Objetivos de Controle	Resultado Obtido	Oportunidades de Melhoria
4	Solicitações de mudanças no ambiente de TI não serem tempestivamente atendidas e/ou não priorizadas de acordo com a criticidade que representam.	Garantir que as solicitações de mudanças sejam monitoradas, a fim de que respostas adequadas e tempestivas sejam dadas às solicitações, e priorizadas de acordo com sua criticidade com critérios pré-definidos.	Não há políticas e procedimento formalizados que determinem as práticas adequadas para o processo de gestão de mudanças, inclusive o acompanhamento de chamados.	Estabelecer uma Norma de Gestão de Mudanças, definindo aspectos como: Processo de monitoramento contínuo das mudanças.

II.3. – Gerenciar Fornecedores – Serviços Terceirizados – Item 2.3.3 do Termo de Referência

Gerenciar serviços relacionados a TI providos por todo o tipo de fornecedores para atender aos requisitos corporativos, incluindo a seleção de fornecedores, gestão de relacionamento, gestão de contratos e revisão/monitoramento do desempenho do fornecedor quanto a sua efetividade e conformidade.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
1	Não cumprimento dos SLA's (níveis de acordo de serviços) estabelecidos	Garantir que o fornecedor esteja cumprindo os SLAs estabelecidos.	Não identificamos um controle de monitoramento em caso de acionamento dos fornecedores "Mr. DBA" e "S&M", bem como critérios de avaliação e plano de ação para casos de não cumprimento dos acordos de níveis de serviços contratados.	Definir acordos de níveis de serviço com todos os fornecedores considerados como críticos e incluí-los no processo de monitoramento de acordos de níveis de serviços. Padronizar e documentar o processo de monitoramento de acordos de níveis de serviço dos fornecedores críticos em relação ao SBE.

II.3. – Gerenciar Fornecedores – Serviços Terceirizados – Item 2.3.3 do Termo de Referência

Gerenciar serviços relacionados a TI providos por todo o tipo de fornecedores para atender aos requisitos corporativos, incluindo a seleção de fornecedores, gestão de relacionamento, gestão de contratos e revisão/monitoramento do desempenho do fornecedor quanto a sua efetividade e conformidade.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
2	Indisponibilidade de serviços críticos ao negócio.	Garantir que existam critérios definidos para monitoramento de desempenho, em alinhamento com os SLAs.	Não identificamos um controle periódico de avaliação de desempenho dos fornecedores Mr.DBA e S&M.	Padronizar e documentar um processo de avaliação de desempenho de fornecedores.

3.1.5. Controle de acesso lógico

III.1 – Gerenciar Segurança de Terminais – Item 2.3.4 do Termo de Referência

Assegurar que os terminais são protegidos em um nível igual ou superior ao requerido pelo nível de criticidade definido para a informação tratada, armazenada ou transmitida.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
1	Utilização da estação de trabalho por terceiros não autorizados.	Assegurar que as estações de trabalho sejam utilizadas apenas por usuários autorizados.	A estação de trabalho observada não sofreu bloqueio automático durante os 15 minutos de inatividade, estando em desconformidade com o item “6.2 de Gerenciamento de Acesso do Usuário”, constante na “Norma de Segurança da Informação para Controle de Acesso” (NO-SC-001-1.1) da companhia. Concluímos, dessa forma, que a estação de trabalho não obedece às diretivas de segurança estabelecidas na Group Policy do Active Directory.	Garantir que todas as estações de trabalho obedeçam aos parâmetros de segurança definidas no GPO (*Group Policy Objective).* É recomendável que as alterações feitas nas configurações de segurança das estações Linux resultem em alertas para a equipe de Segurança e Conformidade. Realizar o *enforcement* da Norma Organizacional de Segurança da Informação para Controle de Acesso.
2	Roubo de informações confidenciais.	Garantir que as informações contidas em dispositivos/mídias de armazenamento de dados descartados não possam ser recuperadas.	Controle Efetivo	Não Aplicável

III.2 – Gerenciar Perfil de Usuários e Acesso Lógico – Item do 2.3.4 do Termo de Referência

Certificar ~~que todo~~s os usuários têm direitos de acesso à informação, de acordo com as suas necessidades de negócios e coordenar com as unidades de negócios que gerem os seus próprios direitos de acesso dentro de processos de negócios.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
1	Descumprimento da política de segurança por parte dos usuários.	Garantir que todos os colaboradores tenham ciência do conteúdo das políticas de segurança da companhia.	Observamos que um usuário recebeu acesso ao ambiente tecnológico da RioCard em 24/06/2014 sem realizar assinatura do termo de responsabilidade de uso.	Reforçar a governança dos controles do processo de gestão de acesso de usuários, para que seja garantida a assinatura do "Termo de Uso Aceitável dos Recursos Computacionais e Comunicação".
2	Acesso não autorizado de usuários aos sistemas de informações, banco de dados e sistema operacional.	Garantir que o processo de concessão e alteração de acesso de usuários aos recursos de TI seja formalmente solicitado, avaliado e aprovado conforme procedimentos previamente definidos e documentados.	Existência da aprovação de um usuário aprovado, no nível de Diretoria, sem que fosse seguido o *workflow* definido de aprovação.	Reforçar a governança dos controles do processo de gestão de acesso de usuários, com o objetivo de assegurar que os acessos sejam tempestivos, formalizados e aprovados pelo gestor designado.
3	Impossibilidade de atribuir responsabilidade por ações realizadas pelos usuários de sistemas, banco de dados e sistema operacional.	Assegurar que todos os usuários cadastrados nos sistemas, banco de dados e sistema operacional, tenham uma conta única e exclusiva, que possa ser utilizada mediante o uso de senha para acesso.	Não identificamos controles de identificação única para os usuários: metro01, metro02, metro10, que são associadas a operadoras, sem um responsável único atribuído.	Incorporar à Política de Gestão de Acesso aspectos como os procedimentos necessários para que usuários e suas atividades nos sistemas sejam unicamente identificáveis.
4	Comprometimento da segurança das informações corporativas devido à falha na autenticação de acesso de	Garantir que os parâmetros de acesso aos sistemas de informações contemplem especificações de segurança, tais como, tamanho mínimo de senha, data de expiração	As parametrizações de senhas do AD e RACF não estão em compliance com a norma da própria RioCard. AD *(Active Directory do Windows)*:	Reforçar aplicação de parâmetros de senha definidos na Norma de Segurança da Informação.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
	usuário nos sistemas de informações.	da senha, padrão de composição de senha, dentre outros.	A política define o bloqueio de senha após 3 tentativas inválidas. O AD não impõe limites para tentativas inválidas. A política define *timeout* após 30 minutos, enquanto no AD está configurado para 600 minutos. RACF A política define o bloqueio de senha após 3 tentativas inválidas. O RACF realiza o bloqueio após 4 tentativas inválidas. Os parâmetros de senha estão sendo adequados à política, com previsão de término em dezembro de 2014.	
5	Uso não autorizado de contas privilegiadas de serviços e aplicações no ambiente tecnológico.	Garantir que o uso de contas de acesso privilegiadas seja restrito e aprovado por alçada competente.	Não foram identificados procedimentos formais de gestão de usuários administradores genéricos	Incorporar à Política de Gestão de Acesso aspectos para a definição de procedimentos relacionados à utilização de superusuários.
6	Comprometimento da segurança das informações corporativas devido à acesso indevido	Garantir que os privilégios de acesso aos sistemas de informações obedecem critérios relacionados á função do colaborador dentro da	Apesar de haver um processo de revisão periódica, ela contempla apenas os acessos de usuários, sem levar em consideração uma revisão dos	Definir mapa de perfis, segregando atividades por papéis funcionais.

III.2 – Gerenciar Perfil de Usuários e Acesso Lógico – Item do 2.3.4 do Termo de Referência

Certificar que todos os usuários têm direitos de acesso à informação, de acordo com as suas necessidades de negócios e coordenar com as unidades de negócios que gerem os seus próprios direitos de acesso dentro de processos de negócios.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
	de usuários aos sistemas de informações.	organização.	perfis. Não há um mapeamento dos perfis e funções conflitantes que deveriam ser consideradas na revisão.	
7	Acesso indevido às informações do sistema SBE e Validador, por uso de conta de usuários inativos.	Assegurar revogação de acesso tempestiva para usuários desligados, em férias ou de licença.	Controle Efetivo	Não Aplicável

3.1.6. Gestão de incidentes de segurança da informação

IV.1 – Gerenciar Requisições de Serviço e Incidentes – Item 2.3.5 do Termo de Referência

Prover resposta e resolução tempestiva e eficaz às solicitações de usuários para todos os tipos de incidentes. Restaurar o serviço normal; Registrar e cumprir todas as solicitações de usuários; e registrar, investigar, diagnosticar, escalar e solucionar incidentes.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
1	Chamados não serem atendidos tempestivamente	Garantir que o tratamento de chamados é feito de maneira tempestiva levando em consideração a urgência e o impacto.	Não identificamos critérios preestabelecidos para classificação da criticidade dos chamados. Atualmente, esta classificação é feita de forma *ad-hoc*[6] por quem assume o chamado.	Definir e documentar critérios para classificação de chamados em relação à sua criticidade. Criar procedimentos para mapeamento e identificação das possíveis causa raiz dos incidentes para evitar a recorrência.
2	Não cumprimento dos SLAs (acordo do nível de serviços) nos prazos estabelecidos	Garantir que os chamados encerrados sejam devidamente tratados.	O monitoramento dos chamados é realizado de forma Ad-Hoc. Não identificamos indicadores de desempenho que apresentem chamados não atendidos e que deverão ser tratados de forma prioritária por conta dos seus SLA's.	Definir e documentar processo e procedimentos de monitoramento dos chamados. Definir e monitorar indicadores de desempenho que apresentem tempo médio de atendimento dos chamados, chamados recorrentes e chamados que não foram atendidos dentro do SLA estabelecido.

---

[6] Ad-Hoc – Conforme conhecimento do usuário, sem um processo e procedimentos definido e documentado.

3.1.7. Aquisição, desenvolvimento e manutenção de sistema de informação.

V.1 – Gerenciar Identificação e Construção de Soluções – Item 2.3.6 do Termo de Referência

Estabelecer e manter soluções identificadas em linha com os requisitos da empresa que abrangem a concepção, desenvolvimento, aquisição/terceirização e parcerias com fornecedores/vendedores. Gerenciar configuração, preparação para testes, testes, gestão e manutenção dos processos de negócio requerimentos, aplicações, informações/dados, infraestrutura e serviços.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
1	Dados dos sistemas de aplicação processados incorretamente.	Garantir a integridade do processamento no ambiente de produção	Não foi identificada a formalização da revisão dos códigos de aplicações e nem a formalização da liberação para produção dos “pacotes de atualização”, para a totalidade de mudanças avaliadas.	Documentar a revisão de código e a liberação para produção dos “pacotes de atualização”. Adicionar ao final da documentação da mudança: a versão final do release e o chamado na Central de Serviços.
2	Não atendimento aos requisitos de negócio.	Assegurar que a solução desenvolvida atende às necessidades da área solicitante.	A área que desenvolve e mantém os sistemas é a mesma que testa/homologa as funcionalidades.	Rastrear mudanças nos requisitos, permitindo que todos os *stakeholders* monitorem, revisem e aprovem as mudanças. Assegurar-se que os resultados do processo de mudanças sejam completamente entendidos e concordados por todos os *stakeholders* e contratante/dono do produto.
3	Interrupções no processamento do ambiente de produção.	Reduzir ocorrência de bugs em ambiente de produção; Mitigar o risco de interrupção do	Controle Efetivo	Não Aplicável

		ambiente de produção;		

V.2 – Gerenciar Acordos de Nível de Serviço – Item 2.3.6 do Termo de Referência

Definir acordo de níveis de serviço de acordo com as necessidades e expectativas da empresa, incluindo a identificação, especificação, projeto, publicação, acordo, e acompanhamento de serviços de TI, níveis de serviço e indicadores de desempenho.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
1	Catálogo de serviços não atendendo as necessidades dos clientes.	Garantir que o catálogo de serviços está de acordo com as necessidades dos clientes e capacidades do negócio.	A Central de Serviços foi iniciada em Outubro de 2013 e, até a data de execução de nossos trabalhos (novembro de 2014), não foi concluída uma revisão do Catálogo de Serviços.	Executar o Processo de Revisão do Catálogo de Serviços dentro do período de 1 (um) ano, considerando os acordos de nível de serviço que deverão ser cumpridos.
2	Serviços não serem entregues aos clientes de forma satisfatória.	Garantir que os serviços são entregues conforme estabelecido entre as partes.	As evidências de plano de ação fornecidas possuem datas anteriores ao envio do relatório, sendo assim, não verificamos relacionamento entre os documentos.	Elaborar e Executar Planos de Ação para tratamento e correções de desvios identificados nas medições do relatório mensal de desempenho.

3.1.8. Gestão da continuidade do negócio

VI.1 – Gerenciar Continuidade – Item 2.3.7 do Termo de Referência

Estabelecer e manter um programa que permita a organização responder a incidentes e interrupções de TI e de negócios, de modo a continuar a operação de processos críticos de negócios e serviços de TI necessários e manter a disponibilidade de informações em um nível aceitável para a empresa.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
1	Incapacidade de recuperar os serviços críticos de TI em tempo hábil, em caso de parada inesperada em decorrência de desastres.	Assegurar que estejam definidos e documentados os procedimentos para continuidade dos serviços críticos de TI que suportam os sistemas SBE e Validador, bem como programas de teste e revisão destes procedimentos.	Não foi identificado um procedimento formalmente documentado, como um Plano de Continuidade de Negócios, que descreva as ações necessárias para reestabelecimento dos ativos críticos de TI em situação de crise ou desastre. A ausência de procedimentos de contingência formalmente documentado pode acarretar em indisponibilidade dos sistemas de Bilhetagem Eletrônica (SBE) e Validador, além da perda de dados, caso algum incidente afete esses sistemas.	Elaborar os manuais operacionais para qualificação e tratamento de incidentes, para casos de interrupção do negócio, não somente associados à segurança da informação. Documentar e implantar o Plano de Continuidade de Negócio (PCN) operacional prevendo processos e pessoas, contendo procedimentos para a operação contínua de processos críticos, incluindo a simulação de cenários de interrupção de TI para testar o plano. Realizar treinamento e conscientização de PCN periodicamente.
2	Incapacidade de recuperar os serviços críticos de TI em tempo hábil, em caso de parada inesperada em	Assegurar a continuidade dos processos críticos de negócio através de um procedimento eficiente de contingência de TI.	Controle Efetivo	Não Aplicável

VI.1 – Gerenciar Continuidade – Item 2.3.7 do Termo de Referência

Estabelecer e manter um programa que permita a organização responder a incidentes e interrupções de TI e de negócios, de modo a continuar a operação de processos críticos de negócios e serviços de TI necessários e manter a disponibilidade de informações em um nível aceitável para a empresa.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
	decorrência de desastres.			
3	Salvaguarda de dados não atender aos requerimentos do negócio (retenção, abrangência, guarda (*in/off-site*), etc)	Assegurar que os requerimentos de salvaguarda de dados, que atendam os requisitos de negócios, estejam definidos, documentados e divulgados.	Os requerimentos de salvaguarda de dados, que atendam os requisitos de negócios, não estão definidos e documentados.	Estabelecer uma Norma de gerenciamento de cópia de segurança (*backup*), que defina, entre outros: frequência, modo de realização do *backup*, tipo de mídia, *backups online* automatizados, tipos de dados, descarte de mídia e segurança.
4	Impossibilidade de recuperar dados processados pelos sistemas de informações, caso ocorra incidente que acarrete a perda de dados.	Garantir que são gerados e mantidos backups periódicos dos dados dos sistemas.	Controle Efetivo	Não Aplicável
5	Impossibilidade de recuperar dados mantidos nas mídias de backup, caso ocorra alguma falha que resulte no dano da mídia ou arquivo gerado durante o backup de dados.	Garantir a realização de procedimentos que atestem a integridade das mídias e arquivos de backups de dados.	Não são realizados testes periódicos nas mídias contendo os backups de dados. A integridade física das mídias são verificadas apenas no momento da (re)utilização das mídias.	Executar procedimento de testes periódicos de *restore* de dados em backup, conforme "NO-SC-004-00- Norma de Segurança da Informação em Operações e Comunicações".
6	Incapacidade de localizar as fitas de backup de forma tempestiva quando	Garantir guarda organizada das mídias contendo o backup de dados, que possibilite a tempestiva	Controle Efetivo	Não Aplicável

VI.1 – Gerenciar Continuidade – Item 2.3.7 do Termo de Referência

Estabelecer e manter um programa que permita a organização responder a incidentes e interrupções de TI e de negócios, de modo a continuar a operação de processos críticos de negócios e serviços de TI necessários e manter a disponibilidade de informações em um nível aceitável para a empresa.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
	necessário a restauração dos dados.	localização e busca, quando necessário.		

VI.2 – Gerenciar Riscos – Item 2.3.7 do Termo de Referência

Continuamente identificar, avaliar e reduzir os riscos relacionados a TI aos limites de níveis de tolerância, estabelecido pela gestão executiva da empresa.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
1	Materialização de riscos não analisados.	Assegurar que a organização tem mapeados os principais riscos aos quais está exposta, e possui uma ação definida para cada risco.	Não identificamos, durante a execução de nossos testes, um processo formalizado para gestão de riscos da organização.	Estabelecer um processo com frequência pré-determinada de análise de riscos e posterior tratamento dos mesmos, com planos de ação formalizados.

3.1.9. *Avaliação dos ambientes e meios físicos onde os diversos componentes do SBE estão dispostos*

VII.1 – Gerenciar Acesso Físico aos Ativos de TI – Item 2.3.9 do Termo de Referência

Definir e implementar procedimentos para conceder, limitar e revogar o acesso as instalações, edifícios e áreas de acordo com as necessidades do negócio, incluindo situações de emergência. O acesso aos locais, edifícios e áreas deve ser justificado, autorizado, registrado e monitorado. Isto deve aplicar-se a todas as pessoas que entram nas instalações, incluindo funcionários, pessoal temporário, clientes, fornecedores, visitantes ou qualquer outro terceiro.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
1	Acesso indevido às instalações que hospedam ativos críticos de TI.	Garantir que somente pessoas autorizadas tenham acesso às dependências do Datacenter.	Não foi possível identificar o registro formal de solicitação e aprovação de acesso ao Datacenter (ausência de ocorrência de nenhum caso no ano de 2014, até a execução de nossos testes). Não há registro dos visitantes. A norma não determina claramente quem são as pessoas autorizadas a ter acesso biométrico permitido ao Datacenter.	Reforçar controles para registro de todos os visitantes que acessarem o *Data Center*, sem autenticação de acesso por biometria.

3.1.10.Avaliação das redes de comunicação

VIII.1 – Gerenciar Segurança de Rede e Conectividade – Item 2.3.10 do Termo de Referência

Utilizar as medidas de segurança e procedimentos de gestão relacionados para proteger as informações sobre todos os métodos de conectividade.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
1	Acesso não autorizado à rede interna da empresa.	Garantir que o acesso ao ambiente de tecnologia da informação da RioCard seja concedido apenas a dispositivos autorizados.	Controle Efetivo	Não Aplicável
2	Acesso não autorizado à rede interna da empresa.	Garantir que o ambiente tecnológico seja capaz de identificar e resistir à ameaças, por meio de mecanismos prevenção de intrusão e detecção de tráfego na rede, como firewall.	Controle Efetivo	Não Aplicável
3	Violações de segurança à rede interna não detectadas em tempo hábil.	Garantir que o ambiente tecnológico seja capaz de identificar e resistir a ameaças, por meio de mecanismos prevenção de intrusão e detecção de tráfego na rede, como IDS.	Controle Efetivo	Não Aplicável
4	Violações de segurança ao ambiente tecnológico não sejam detectadas em tempo hábil, nas aplicações *web*.	Garantir que o ambiente tecnológico seja capaz de identificar e resistir a ameaças que possam expor as informações da empresa à	*Ambiente Valorado* Não foram identificadas exceções.	*Ambiente Valorado* Não Aplicável

VIII.1 – Gerenciar Segurança de Rede e Conectividade – Item 2.3.10 do Termo de Referência

Utilizar as medidas de segurança e procedimentos de gestão relacionados para proteger as informações sobre todos os métodos de conectividade.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
		acessos não autorizados.	*Ambiente de Gratuidade* Identificamos que dados sensíveis, como informações de *login* e senha, estão sendo transmitidos através de um canal não criptografado. O *web server* se encontra configurado para mostrar a lista de arquivos contidos em seus diretórios, dentre esses arquivos podem estar contidos diversas informações que podem ser confidenciais ou podem ser utilizadas para gerar um ataque mais sofisticado a esse servidor. Através das páginas acessíveis pela listagem de diretório, é possível criar usuários e/ou alterar dados de usuários existentes.	*Ambiente de Gratuidade* Recomendamos que as informações sensíveis sejam trafegadas por conexões criptografadas (HTTPS) para que os dados não sejam interceptados por um usuário malicioso. Avaliar a efetiva necessidade da listagem de arquivos, com o objetivo de garantir que esses arquivos não exponham informações que possam ser utilizadas por um usuário mal intencionado. Recomendamos que não seja possível habilitar a listagem de diretórios nas configurações do *web server*. É recomendável que se use restrição de permissão para que visitantes não visualizem e alterem informações restritas.

VIII.1 – Gerenciar Segurança de Rede e Conectividade – Item 2.3.10 do Termo de Referência

Utilizar as medidas de segurança e procedimentos de gestão relacionados para proteger as informações sobre todos os métodos de conectividade.

ID	Riscos	Objetivos de Controle	Resultado	Oportunidades de Melhoria
5	Regras de segurança aplicadas ou modificadas nos dispositivos tecnológicos em desacordo com a política de segurança da informação.	Garantir que apenas modificações autorizadas sejam realizadas em regras de dispositivos de segurança.	Controle Efetivo	Não Aplicável
6	Acesso não autorizado às informações da empresa, durante a transmissão e recepção de dados.	Aplicar mecanismos confiáveis para assegurar a proteção dos dados transmitidos e recebidos por meio do uso da internet pública.	Controle Efetivo	Não Aplicável

4. Testes de Intrusão

Os testes de intrusão (interno e externo) referem-se ao item 2.3.8 do Termo de Referência e encontram-se detalhados a seguir.

4.1. Teste externo de intrusão em aplicação web e infraestrutura

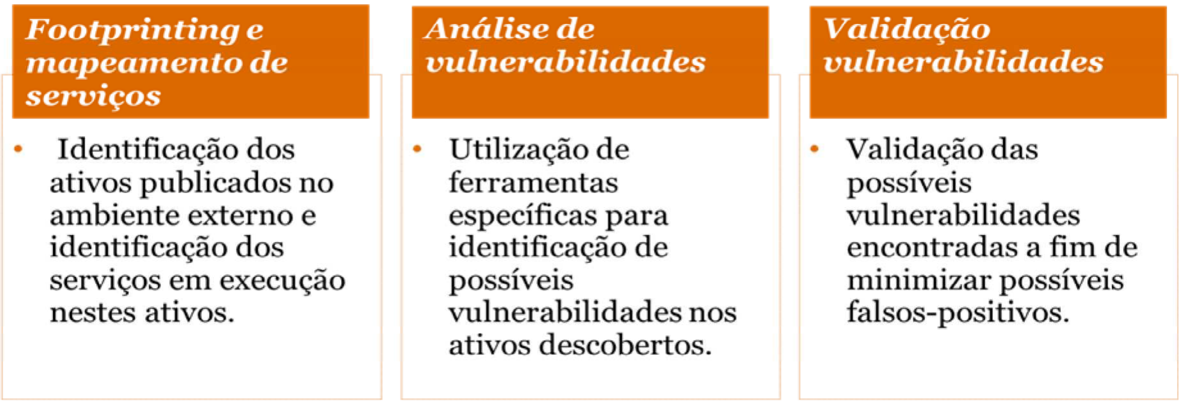
4.1.1. Abordagem e escopo do Projeto para o teste de intrusão externo

Abordagem adotada

Em conformidade com os parâmetros especificados para a realização dos testes, recebemos os endereços dos sites e serviços utilizados pela RioCard, conforme tabela a seguir:

Hosts avaliados	IPs
http://www.vt.fetranspor.com.br/operadoras/	192.230.74.73
https://www.cartaoriocard.com.br	199.83.135.7
http://www.riocard.com	199.83.135.200
Concentrador de VPN (1)	200.201.148.243
Concentrador de VPN (2)	200.201.145.2
Servidor FTP	200.201.145.63

A seguir, apresentaremos as etapas, as técnicas utilizadas para análise e exploração de vulnerabilidades utilizadas para testar a segurança dos endereços pertencentes ao escopo.



Footprinting e mapeamento de serviços

- Identificação dos ativos publicados no ambiente externo e identificação dos serviços em execução nestes ativos.

Análise de vulnerabilidades

- Utilização de ferramentas específicas para identificação de possíveis vulnerabilidades nos ativos descobertos.

Validação vulnerabilidades

- Validação das possíveis vulnerabilidades encontradas a fim de minimizar possíveis falsos-positivos.

As seguintes ferramentas foram utilizadas para a execução dos nossos testes: (a) Acunetix; (b) Burp Suite; (c) Nessus; (d) Nmap; e (e) Kali Linux.

Classificação das vulnerabilidades

Para cada vulnerabilidade as mesmas foram classificadas conforme critério de severidade descrito na tabela a seguir:

Severidade	*Descrição*
Crítica	Vulnerabilidades as quais permitiram o comprometimento lógico da segurança do sistema avaliado. Na maioria dos casos, a exploração desta vulnerabilidade permitirá ao atacante acesso administrativo ao sistema afetado e permite a realização de ataques que tornariam o sistema ou seus dados inutilizáveis. Um usuário mal intencionado pode obter informações altamente sensíveis, que se divulgados, poderiam causar danos consideráveis a empresa. Neste caso, a segurança do sistema ou da rede pode ser totalmente comprometida.
Alta	Incluem vulnerabilidades as quais podem permitir o comprometimento lógico da segurança do sistema avaliado. Um usuário mal intencionado poderia obter controle interativo, por exemplo, uma conta do usuário através de força bruta, ou o controle do sistema através de um serviço de baixo privilégio. Pode permitir um usuário mal intencionado acessar informações (como dados do cliente) no sistema avaliado.
Média	Vulnerabilidades que não comprometem diretamente o sistema ou os dados, mas que poderiam ser utilizadas para ganhar um acesso adicional. Isto poderia incluir *exploits* locais para aumentar privilégio (por exemplo, um usuário se tornar um administrador), à falta de segurança nos dados (por exemplo, falta de criptografia em arquivos confidenciais ou comunicações de rede). Esses poderiam ser usados como vetores de ataques. Vulnerabilidades que podem exclusivamente causar negação de serviço (*DoS – Denial of Service*) sem o comprometimento de dados também são classificadas como de nível médio.
Baixa	Vulnerabilidades de nível baixo podem permitir o vazamento de informações, como por exemplo, a coleta de informações estatísticas de sistema, nomes de usuários, informações de endereçamento interno, informações sobre a organização ou sistemas, que normalmente são utilizadas para a construção de ataques mais sofisticados.

4.1.2. Resultados Obtidos

Durante a realização dos testes automatizados de aplicação *web*, foram executadas 330 verificações em cada uma das três aplicações em escopo.

Além dos testes automatizados, foram realizados testes manuais nas três aplicações em escopo. Para executar esses testes manuais, também foram utilizados os resultados dos testes automatizados, a fim de validar as principais vulnerabilidades encontradas.

Tabela 3 – Detalhe das vulnerabilidades encontradas nas aplicações web (vide detalhamento das vulnerabilidades no Anexo C – Matriz de Vulnerabilidades de Aplicação web)

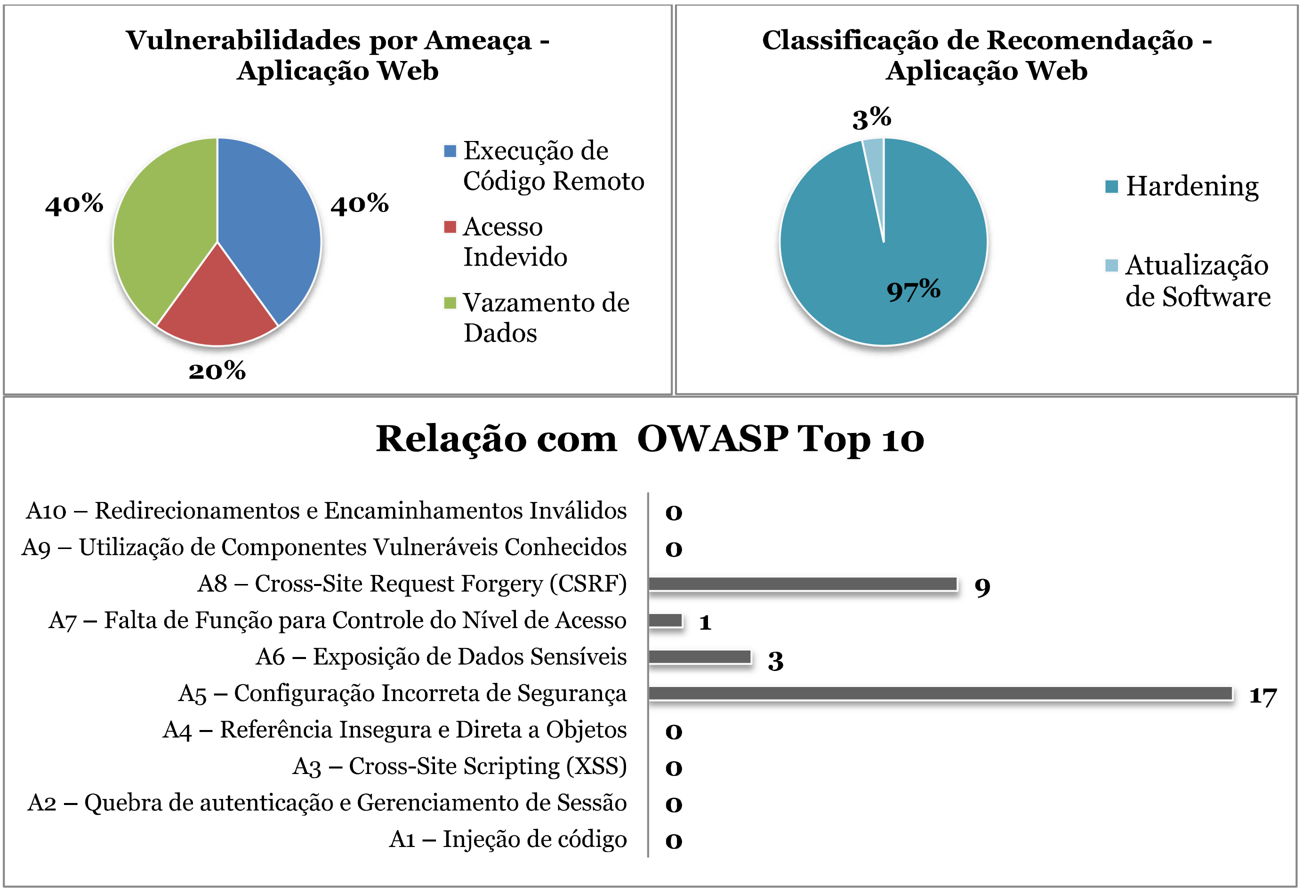
Severidade	**Vulnerabilidade**	**Site (1)**	**Site (2)**	**Site (3)**	**Total**
Crítica	Failure to Restrict URL Access	1	-	-	1
Alta	Cleartext submission of password	1	1	-	2
Média	Directory Listing	6	-	-	17
	HTML form without CSRF protection	4	-	5	
	TLS1/SSLv3 Renegotiation Vulnerability	-	-	1	
	CAPTCHA Validation in the Client Side	1	-	-	
Baixa	Clickjacking: X-Frame-Options header missing	1	1	1	10
	OPTIONS method is enabled	1	1	1	
	Session Cookie without HttpOnly flag set	1	1	-	
	Session Cookie without Secure flag set	1	1	-	
Total		**17**	**5**	**8**	**30**

Sites avaliados:

1. *Gratuidade: www.riocard.com*
2. *Operadoras: www.vt.fetranspor.com.br/operadoras*
3. *Valorado: www.cartaoriocard.com.br*

Adicionalmente, mapeamos os tipos de ameaças relacionadas às vulnerabilidades encontradas, classificação de recomendação para corrigi-las e também as relacionamos com o OWASP Top 10[7] (*vide gráfico 1*).

Gráfico 1 - Vulnerabilidades encontradas relacionadas com o OWASP Top 10



---

[7] OWASP: *The Open Web Application Security Project* é uma comunidade aberta dedicada para habilitar Organizações para desenvolver, comprar e manter aplicações que devem ser confiáveis.

Durante a realização dos testes automatizados de infraestrutura, foram avaliadas **67.434** vulnerabilidades distribuídas em **50** categorias. Os testes foram realizados para as três aplicações web, os dois concentradores de VPN e o servidor FTP em escopo. A ***tabela 4*** abaixo detalha as **6** vulnerabilidades encontradas infraestrutura em escopo.

Tabela 4 – Detalhe das vulnerabilidades encontradas em ativos de infraestrutura (vide detalhe no anexo D – Matriz de Vulnerabilidades de Infraestrutura)

Severidade	Vulnerabilidade	Ativo 1	Ativo 2	Ativo 3	Ativo 4	Ativo 5	Total
Média	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	-	-	-	1	-	3
	SSL Certificate Cannot Be Trusted	1	1	-	-	-	
Baixa	Disclosure of Personal Information	-	-	1	1	1	3
Total		**1**	**1**	**1**	**2**	**1**	**6**

Infraestrutura avaliada:

Ativo 1: IP - 192.230.74.73
Ativo 2: IP – 199.83.135.200
Ativo 3: IP – 200.201.148.243
Ativo 4: IP – 200.201.145.2
Ativo 5: IP – 200.201.145.63

Resultado do Footprinting

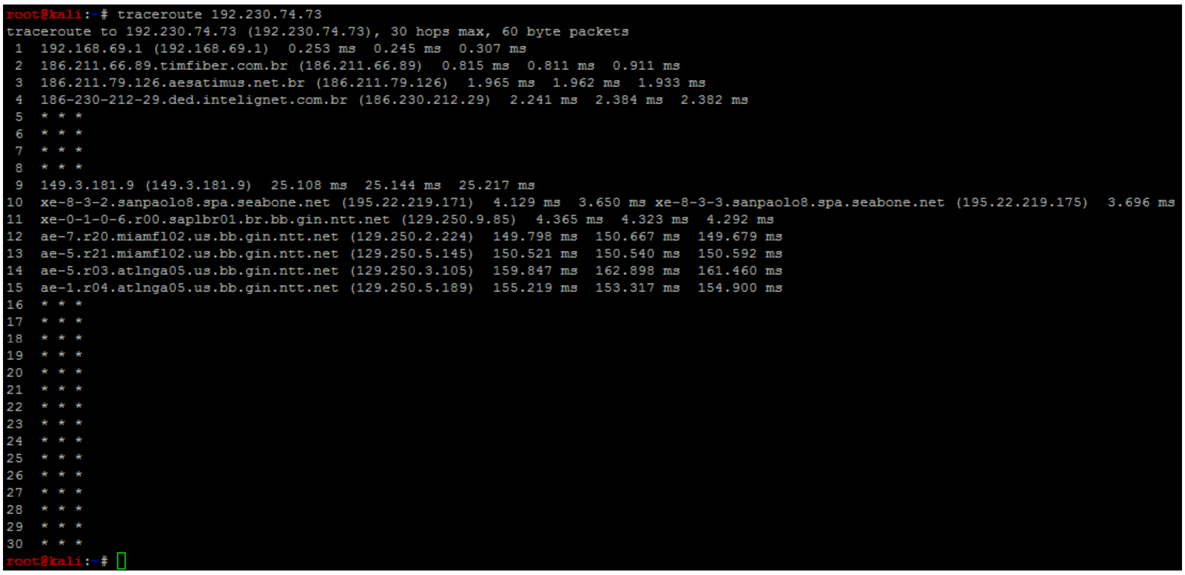
A atividade de Footprinting realizada durante nosso projeto tem como objetivo obter informações que um atacante possa utilizada durante a tentativa de um ataque ao ambiente tecnológico da RioCard. São levantadas informações públicas que estão disponíveis na Internet.

Apresentamos abaixo as etapas e informações obtidas durante a etapa de *Footprinting*.

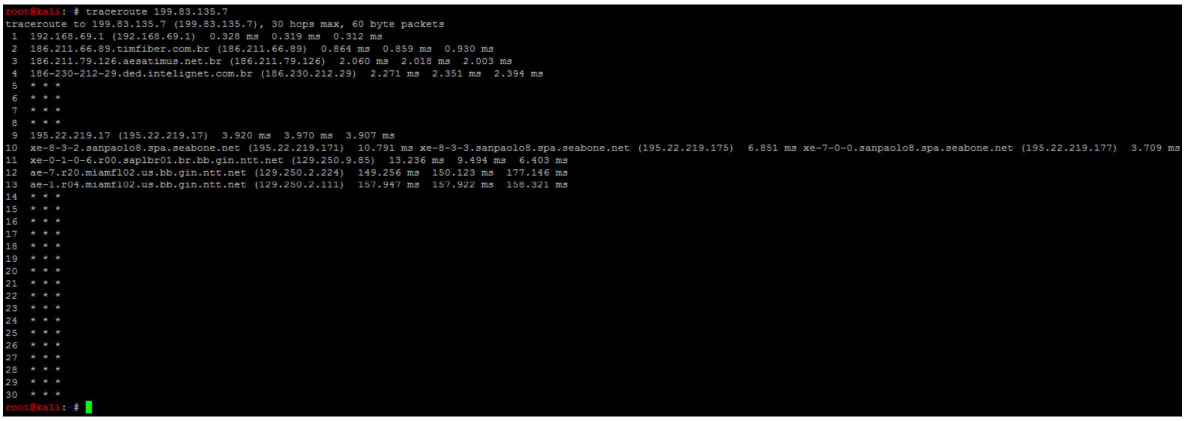
1) Execução do comando *traceroute*

Objetivo: identificação da rota da origem ao destino dos pacotes.

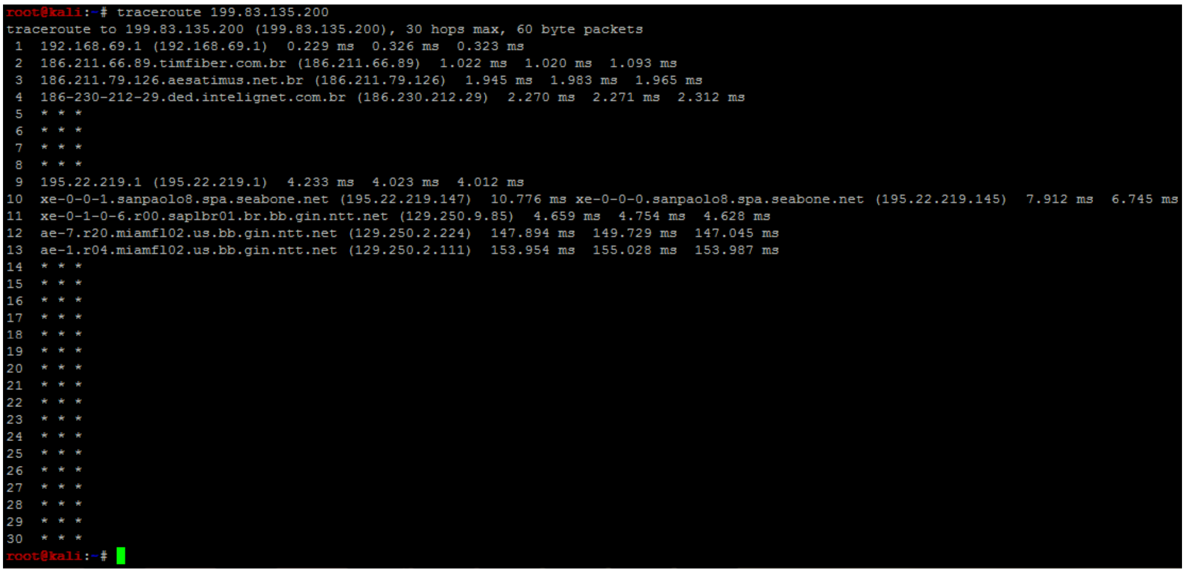
IPs: 199.83.134.73, 199.83.134.7, 199.83.134.200, 200.201.148.243, 200.201.145.2, 200.201.145.63



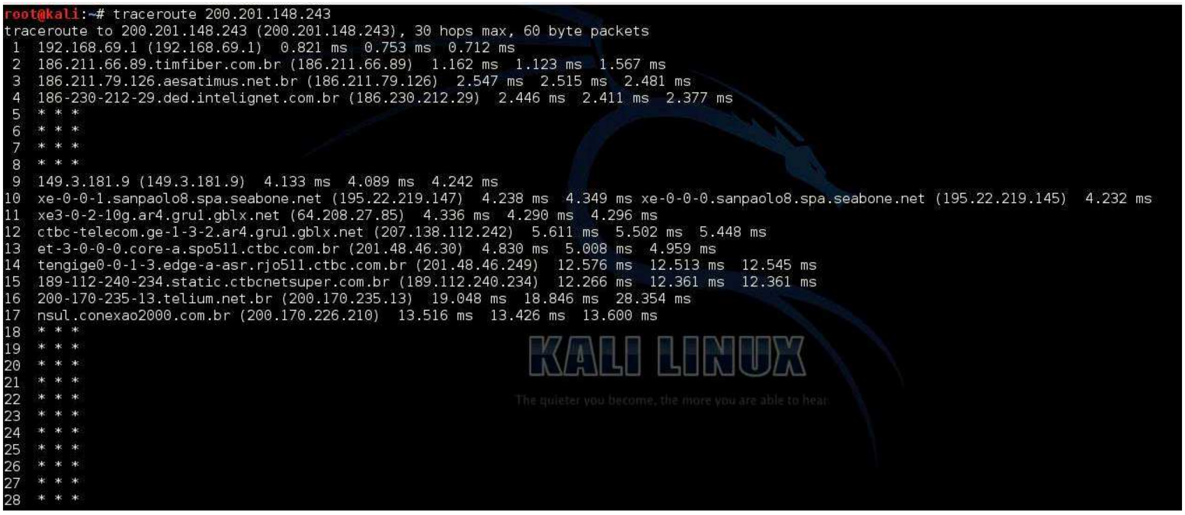
```
root@kali:~# traceroute 192.230.74.73
traceroute to 192.230.74.73 (192.230.74.73), 30 hops max, 60 byte packets
 1  192.168.69.1 (192.168.69.1)  0.253 ms  0.245 ms  0.307 ms
 2  186.211.66.89.timfiber.com.br (186.211.66.89)  0.815 ms  0.811 ms  0.911 ms
 3  186.211.79.126.aesatimus.net.br (186.211.79.126)  1.965 ms  1.962 ms  1.933 ms
 4  186-230-212-29.ded.intelignet.com.br (186.230.212.29)  2.241 ms  2.384 ms  2.382 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  149.3.181.9 (149.3.181.9)  25.108 ms  25.144 ms  25.217 ms
10  xe-8-3-2.sanpaolo8.spa.seabone.net (195.22.219.171)  4.129 ms  3.650 ms xe-8-3-3.sanpaolo8.spa.seabone.net (195.22.219.175)  3.696 ms
11  xe-0-1-0-6.r00.saplbr01.br.bb.gin.ntt.net (129.250.9.85)  4.365 ms  4.323 ms  4.292 ms
12  ae-7.r20.miamfl02.us.bb.gin.ntt.net (129.250.2.224)  149.798 ms  150.667 ms  149.679 ms
13  ae-5.r21.miamfl02.us.bb.gin.ntt.net (129.250.5.145)  150.521 ms  150.540 ms  150.592 ms
14  ae-5.r03.atlnga05.us.bb.gin.ntt.net (129.250.3.105)  159.847 ms  162.898 ms  161.460 ms
15  ae-1.r04.atlnga05.us.bb.gin.ntt.net (129.250.5.189)  155.219 ms  153.317 ms  154.900 ms
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
root@kali:~# 
```



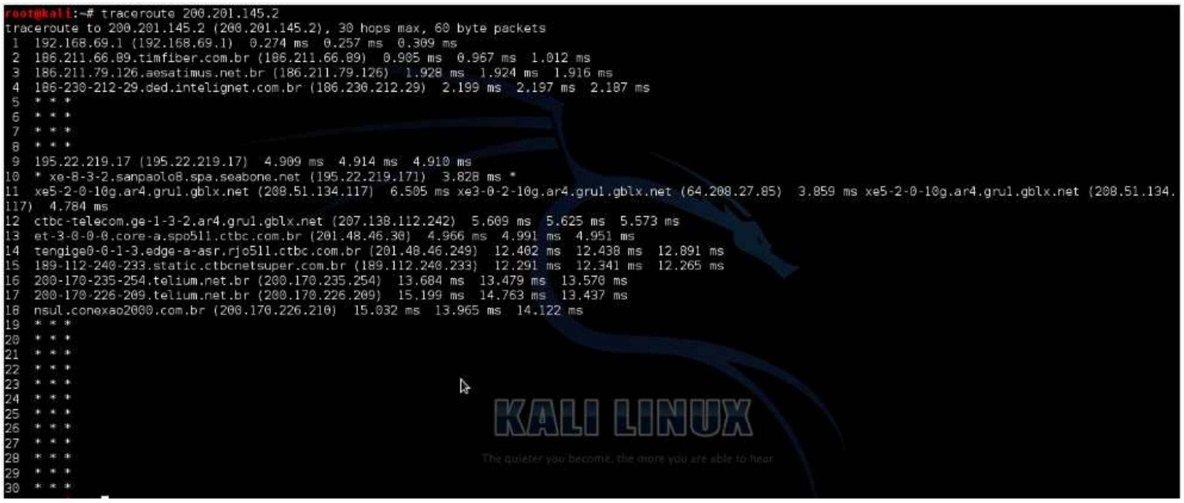
```
root@kali:~# traceroute 199.83.135.7
traceroute to 199.83.135.7 (199.83.135.7), 30 hops max, 60 byte packets
 1  192.168.69.1 (192.168.69.1)  0.328 ms  0.319 ms  0.312 ms
 2  186.211.66.89.timfiber.com.br (186.211.66.89)  0.864 ms  0.859 ms  0.930 ms
 3  186.211.79.126.aesatimus.net.br (186.211.79.126)  2.060 ms  2.018 ms  2.003 ms
 4  186-230-212-29.ded.intelignet.com.br (186.230.212.29)  2.271 ms  2.351 ms  2.394 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  195.22.219.17 (195.22.219.17)  3.920 ms  3.970 ms  3.907 ms
10  xe-8-3-2.sanpaolo8.spa.seabone.net (195.22.219.171)  10.791 ms xe-8-3-3.sanpaolo8.spa.seabone.net (195.22.219.175)  6.851 ms xe-7-0-0.sanpaolo8.spa.seabone.net (195.22.219.177)  3.709 ms
11  xe-0-1-0-6.r00.saplbr01.br.bb.gin.ntt.net (129.250.9.85)  13.236 ms  9.494 ms  6.403 ms
12  ae-7.r20.miamfl02.us.bb.gin.ntt.net (129.250.2.224)  149.256 ms  150.123 ms  177.146 ms
13  ae-1.r04.miamfl02.us.bb.gin.ntt.net (129.250.2.111)  157.947 ms  157.922 ms  158.321 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
root@kali:~# 
```



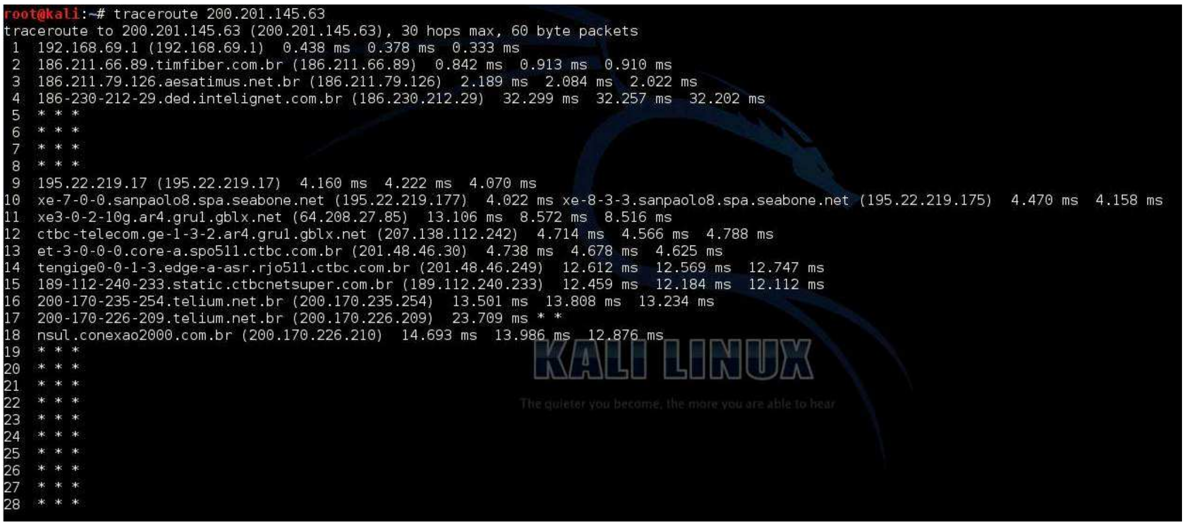
```
root@kali:~# traceroute 199.83.135.200
traceroute to 199.83.135.200 (199.83.135.200), 30 hops max, 60 byte packets
 1  192.168.69.1 (192.168.69.1)  0.229 ms  0.326 ms  0.323 ms
 2  186.211.66.89.timfiber.com.br (186.211.66.89)  1.022 ms  1.020 ms  1.093 ms
 3  186.211.79.126.aesatimus.net.br (186.211.79.126)  1.945 ms  1.983 ms  1.965 ms
 4  186-230-212-29.ded.intelignet.com.br (186.230.212.29)  2.270 ms  2.271 ms  2.312 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  195.22.219.1 (195.22.219.1)  4.233 ms  4.023 ms  4.012 ms
10  xe-0-0-1.sanpaolo8.spa.seabone.net (195.22.219.147)  10.776 ms xe-0-0-0.sanpaolo8.spa.seabone.net (195.22.219.145)  7.912 ms  6.745 ms
11  xe-0-1-0-6.r00.saplbr01.br.bb.gin.ntt.net (129.250.9.85)  4.659 ms  4.754 ms  4.628 ms
12  ae-7.r20.miamfl02.us.bb.gin.ntt.net (129.250.2.224)  147.894 ms  149.729 ms  147.045 ms
13  ae-1.r04.miamfl02.us.bb.gin.ntt.net (129.250.2.111)  153.954 ms  155.028 ms  153.987 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
root@kali:~# 
```



```
root@kali:~# traceroute 200.201.148.243
traceroute to 200.201.148.243 (200.201.148.243), 30 hops max, 60 byte packets
 1  192.168.69.1 (192.168.69.1)  0.821 ms  0.753 ms  0.712 ms
 2  186.211.66.89.timfiber.com.br (186.211.66.89)  1.162 ms  1.123 ms  1.567 ms
 3  186.211.79.126.aesatimus.net.br (186.211.79.126)  2.547 ms  2.515 ms  2.481 ms
 4  186-230-212-29.ded.intelignet.com.br (186.230.212.29)  2.446 ms  2.411 ms  2.377 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  149.3.181.9 (149.3.181.9)  4.133 ms  4.089 ms  4.242 ms
10  xe-0-0-1.sanpaolo8.spa.seabone.net (195.22.219.147)  4.238 ms  4.349 ms xe-0-0-0.sanpaolo8.spa.seabone.net (195.22.219.145)  4.232 ms
11  xe3-0-2-10g.ar4.gru1.gblx.net (64.208.27.85)  4.336 ms  4.290 ms  4.296 ms
12  ctbc-telecom.ge-1-3-2.ar4.gru1.gblx.net (207.138.112.242)  5.611 ms  5.502 ms  5.448 ms
13  et-3-0-0-0.core-a.spo511.ctbc.com.br (201.48.46.30)  4.830 ms  5.008 ms  4.959 ms
14  tengige0-0-1-3.edge-a-asr.rjo511.ctbc.com.br (201.48.46.249)  12.576 ms  12.513 ms  12.545 ms
15  189-112-240-234.static.ctbcnetsuper.com.br (189.112.240.234)  12.266 ms  12.361 ms  12.361 ms
16  200-170-235-13.telium.net.br (200.170.235.13)  19.048 ms  18.846 ms  28.354 ms
17  nsul.conexao2000.com.br (200.170.226.210)  13.516 ms  13.426 ms  13.600 ms
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
```



```
root@kali:~# traceroute 200.201.145.2
traceroute to 200.201.145.2 (200.201.145.2), 30 hops max, 60 byte packets
 1  192.168.69.1 (192.168.69.1)  0.274 ms  0.257 ms  0.309 ms
 2  186.211.66.89.timfiber.com.br (186.211.66.89)  0.905 ms  0.967 ms  1.012 ms
 3  186.211.79.126.aesatimus.net.br (186.211.79.126)  1.928 ms  1.924 ms  1.916 ms
 4  186-230-212-29.ded.intelignet.com.br (186.230.212.29)  2.199 ms  2.197 ms  2.187 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  195.22.219.17 (195.22.219.17)  4.909 ms  4.914 ms  4.910 ms
10  * xe-8-3-2.sanpaolo8.spa.seabone.net (195.22.219.171)  3.828 ms *
11  xe5-2-0-10g.ar4.gru1.gblx.net (208.51.134.117)  6.505 ms xe3-0-2-10g.ar4.gru1.gblx.net (64.208.27.85)  3.859 ms xe5-2-0-10g.ar4.gru1.gblx.net (208.51.134.
117)  4.784 ms
12  ctbc-telecom.ge-1-3-2.ar4.gru1.gblx.net (207.138.112.242)  5.609 ms  5.625 ms  5.573 ms
13  et-3-0-0-0.core-a.spo511.ctbc.com.br (201.48.46.30)  4.966 ms  4.991 ms  4.951 ms
14  tengige0-0-1-3.edge-a-asr.rjo511.ctbc.com.br (201.48.46.249)  12.402 ms  12.438 ms  12.891 ms
15  189-112-240-233.static.ctbcnetsuper.com.br (189.112.240.233)  12.291 ms  12.341 ms  12.265 ms
16  200-170-235-254.telium.net.br (200.170.235.254)  13.684 ms  13.479 ms  13.570 ms
17  200-170-226-209.telium.net.br (200.170.226.209)  15.199 ms  14.763 ms  13.437 ms
18  nsul.conexao2000.com.br (200.170.226.210)  15.032 ms  13.965 ms  14.122 ms
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```



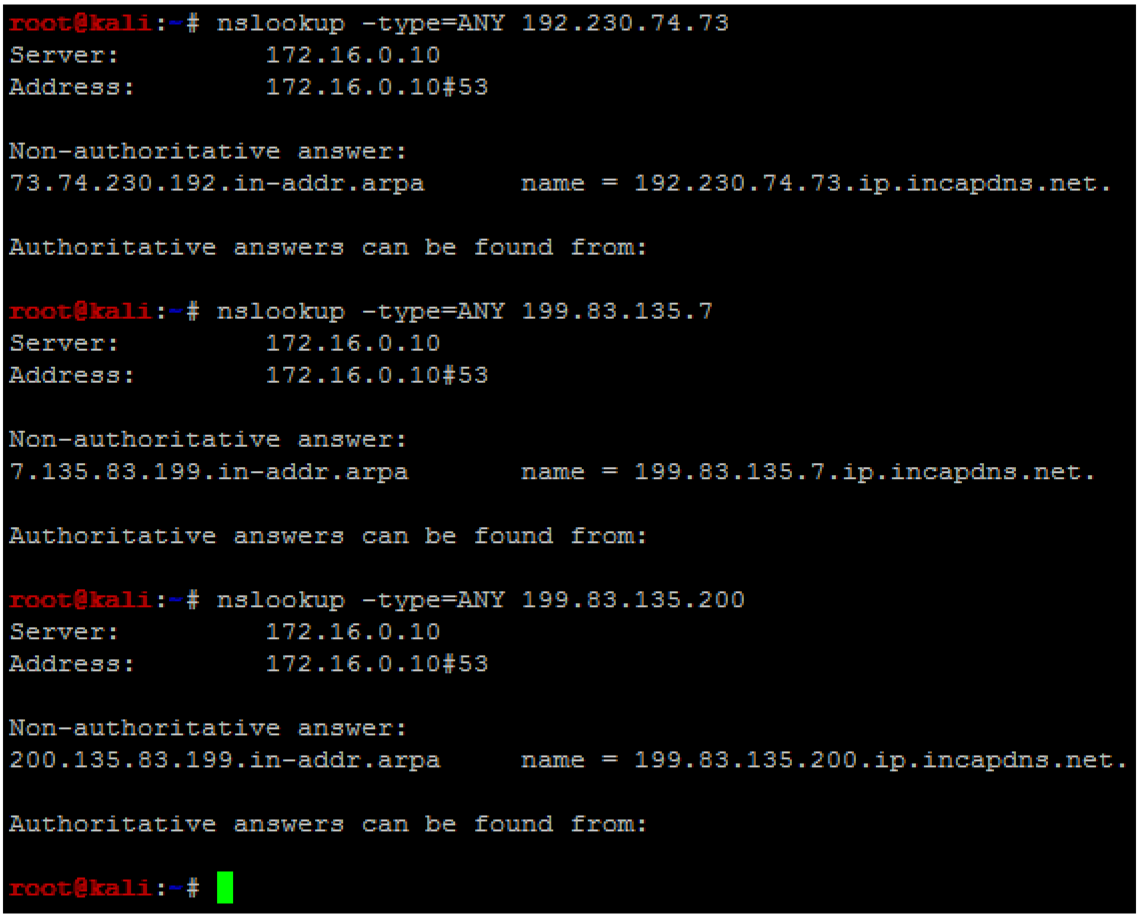
```
root@kali:~# traceroute 200.201.145.63
traceroute to 200.201.145.63 (200.201.145.63), 30 hops max, 60 byte packets
 1  192.168.69.1 (192.168.69.1)  0.438 ms  0.378 ms  0.333 ms
 2  186.211.66.89.timfiber.com.br (186.211.66.89)  0.842 ms  0.913 ms  0.910 ms
 3  186.211.79.126.aesatimus.net.br (186.211.79.126)  2.189 ms  2.084 ms  2.022 ms
 4  186-230-212-29.ded.intelignet.com.br (186.230.212.29)  32.299 ms  32.257 ms  32.202 ms
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  195.22.219.17 (195.22.219.17)  4.160 ms  4.222 ms  4.070 ms
10  xe-7-0-0.sanpaolo8.spa.seabone.net (195.22.219.177)  4.022 ms xe-8-3-3.sanpaolo8.spa.seabone.net (195.22.219.175)  4.470 ms  4.158 ms
11  xe3-0-2-10g.ar4.gru1.gblx.net (64.208.27.85)  13.106 ms  8.572 ms  8.516 ms
12  ctbc-telecom.ge-1-3-2.ar4.gru1.gblx.net (207.138.112.242)  4.714 ms  4.566 ms  4.788 ms
13  et-3-0-0-0.core-a.spo511.ctbc.com.br (201.48.46.30)  4.738 ms  4.678 ms  4.625 ms
14  tengige0-0-1-3.edge-a-asr.rjo511.ctbc.com.br (201.48.46.249)  12.612 ms  12.569 ms  12.747 ms
15  189-112-240-233.static.ctbcnetsuper.com.br (189.112.240.233)  12.459 ms  12.184 ms  12.112 ms
16  200-170-235-254.telium.net.br (200.170.235.254)  13.501 ms  13.808 ms  13.234 ms
17  200-170-226-209.telium.net.br (200.170.226.209)  23.709 ms * *
18  nsul.conexao2000.com.br (200.170.226.210)  14.693 ms  13.986 ms  12.876 ms
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
```

Resultados Obtidos: Foi possível identificar a rota por onde trafegam os pacotes até o mesmo chegar ao seu destino final.

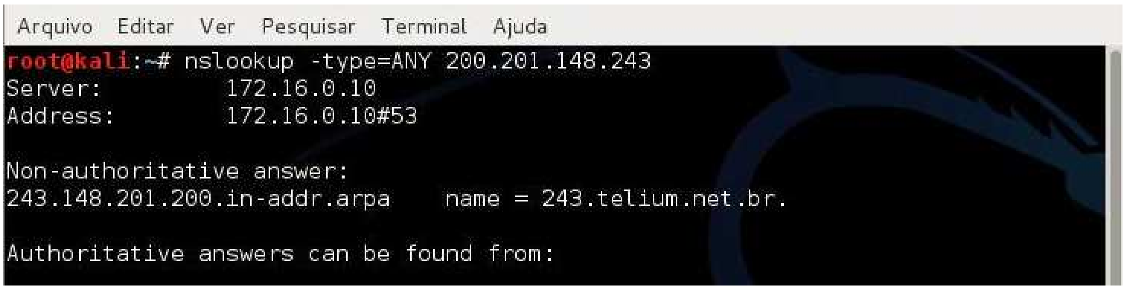
2) Execução do comando nslookup

Objetivo: identificar informações de endereçamento IP, host ou domínio sobre registros de DNS.

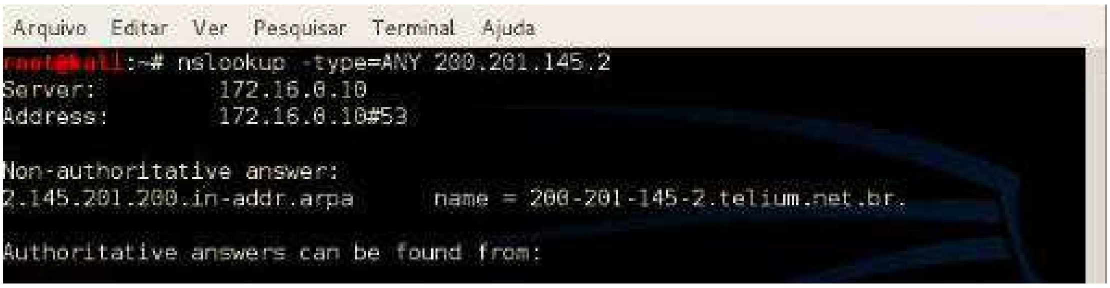
IPs: 199.83.134.73, 199.83.134.7, 199.83.134.200, 200.201.148.243, 200.201.145.2, 200.201.145.63



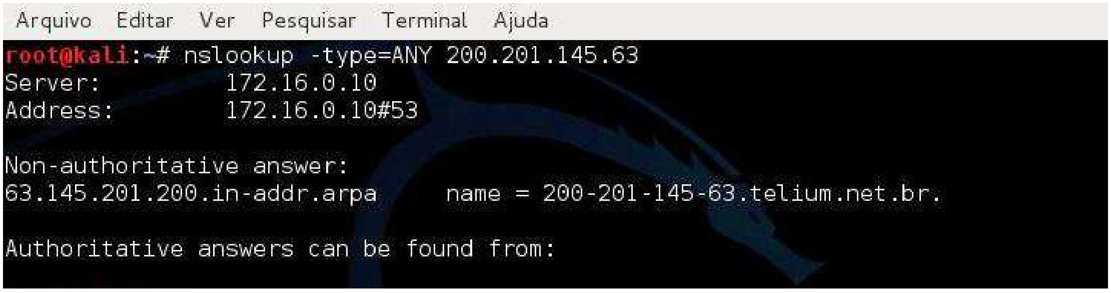
```
root@kali:~# nslookup -type=ANY 192.230.74.73
Server:         172.16.0.10
Address:        172.16.0.10#53

Non-authoritative answer:
73.74.230.192.in-addr.arpa      name = 192.230.74.73.ip.incapdns.net.

Authoritative answers can be found from:

root@kali:~# nslookup -type=ANY 199.83.135.7
Server:         172.16.0.10
Address:        172.16.0.10#53

Non-authoritative answer:
7.135.83.199.in-addr.arpa       name = 199.83.135.7.ip.incapdns.net.

Authoritative answers can be found from:

root@kali:~# nslookup -type=ANY 199.83.135.200
Server:         172.16.0.10
Address:        172.16.0.10#53

Non-authoritative answer:
200.135.83.199.in-addr.arpa     name = 199.83.135.200.ip.incapdns.net.

Authoritative answers can be found from:

root@kali:~# 
```



```
root@kali:~# nslookup -type=ANY 200.201.148.243
Server:         172.16.0.10
Address:        172.16.0.10#53

Non-authoritative answer:
243.148.201.200.in-addr.arpa    name = 243.telium.net.br.

Authoritative answers can be found from:
```


Arquivo
Editar
Ver
Pesquisar
Terminal
Ajuda

```
root@kali:~# nslookup -type=ANY 200.201.145.2
Server:         172.16.0.10
Address:        172.16.0.10#53

Non-authoritative answer:
2.145.201.200.in-addr.arpa      name = 200-201-145-2.telium.net.br.

Authoritative answers can be found from:
```


Arquivo
Editar
Ver
Pesquisar
Terminal
Ajuda

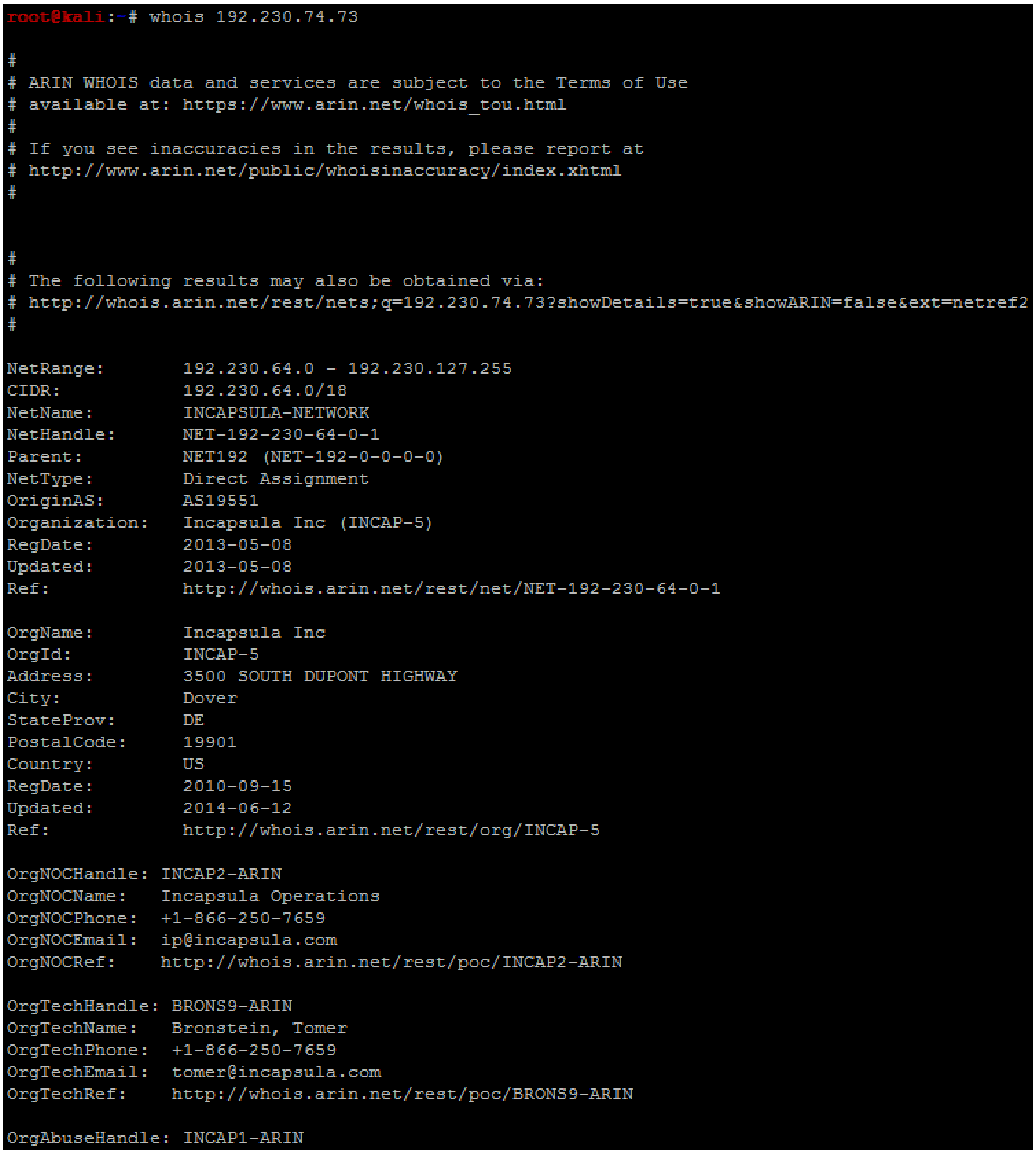
```
root@kali:~# nslookup -type=ANY 200.201.145.63
Server:         172.16.0.10
Address:        172.16.0.10#53

Non-authoritative answer:
63.145.201.200.in-addr.arpa     name = 200-201-145-63.telium.net.br.

Authoritative answers can be found from:
```

Resultados Obtidos: Foi possível identificar os endereços IP dos servidores de DNS.

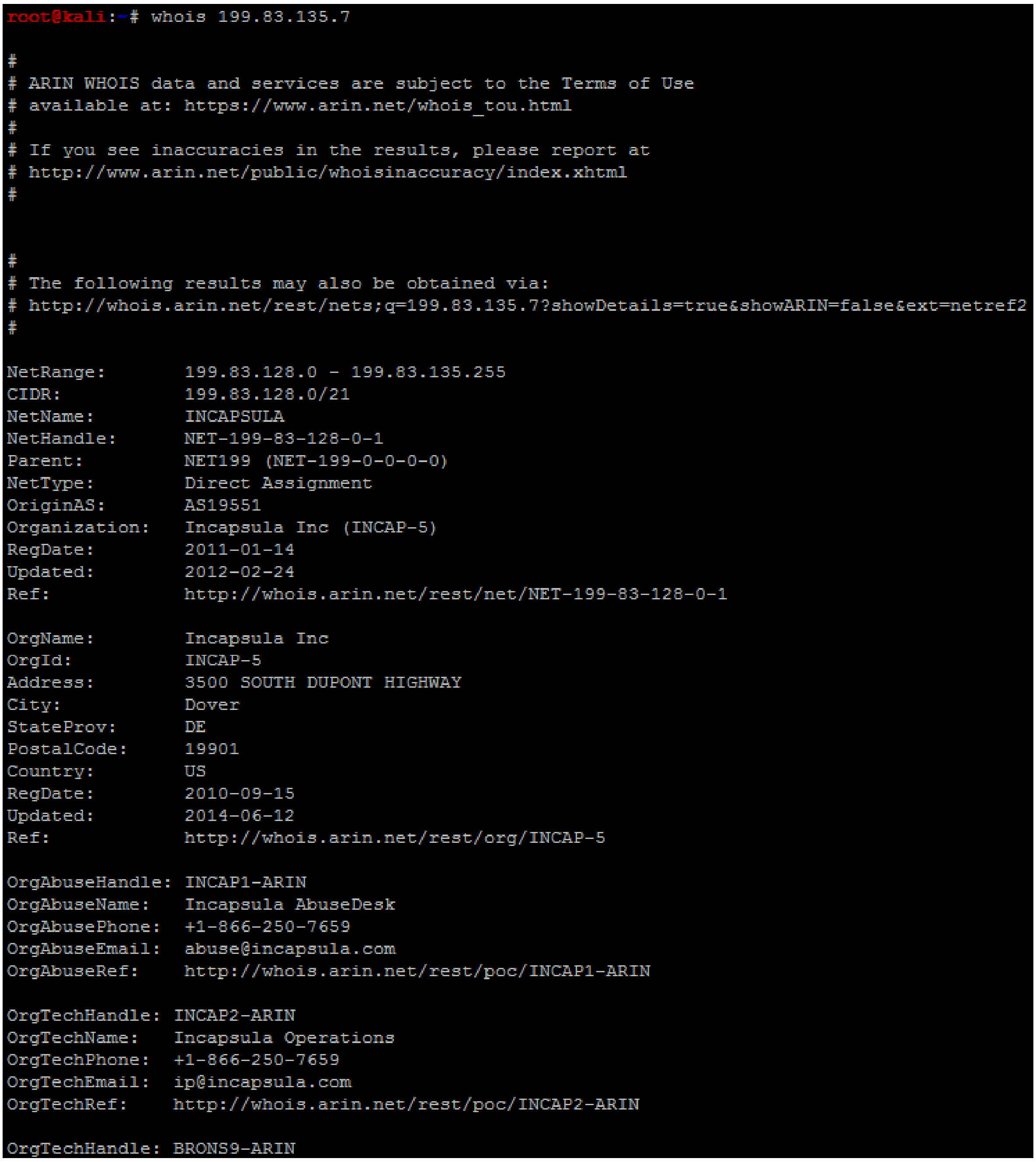
3) Execução do comando Whois

Objetivo: Consultar informações de contato e DNS sobre entidades na internet.

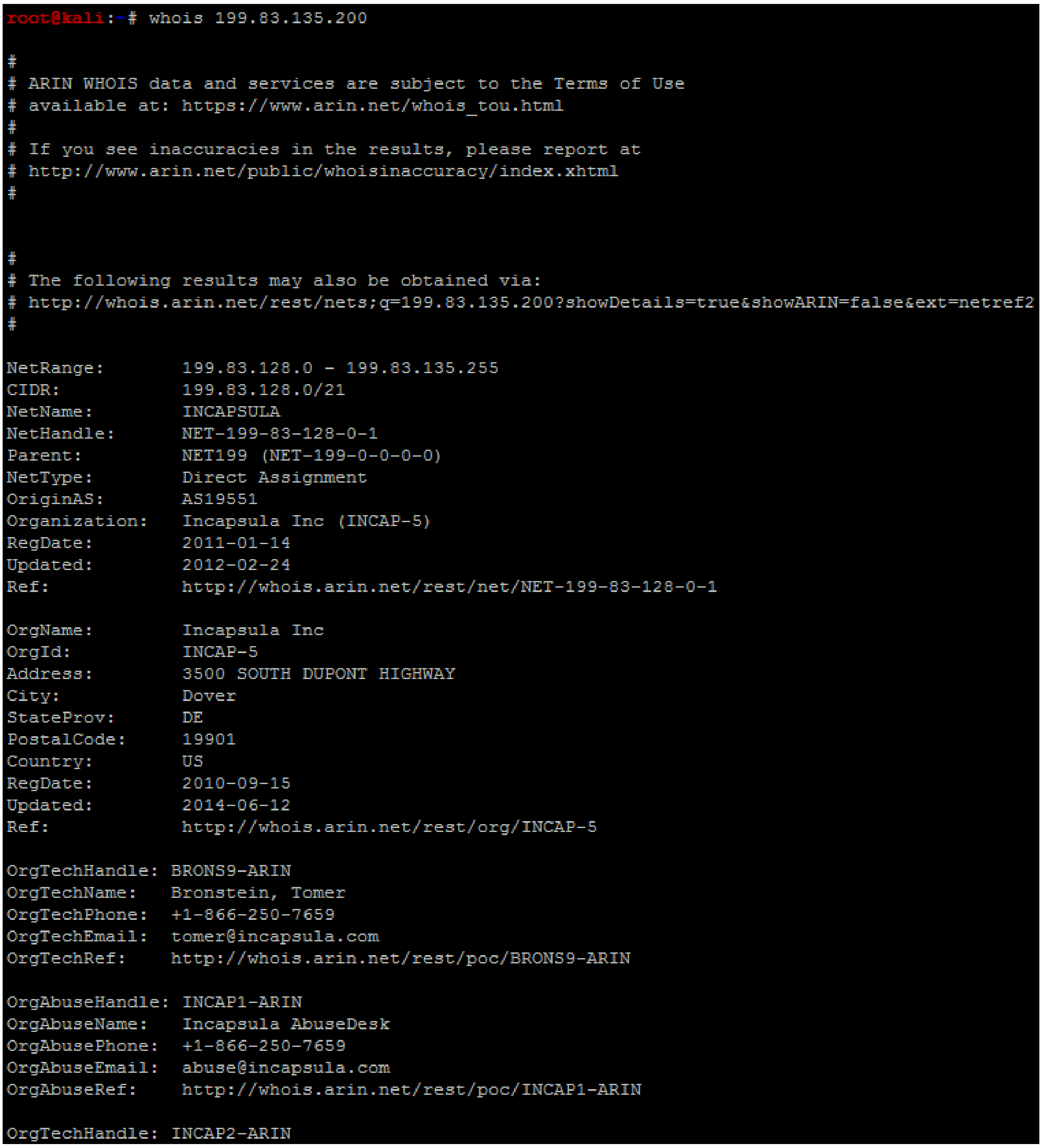
IPs: 199.83.134.73, 199.83.134.7, 199.83.134.200, 200.201.148.243, 200.201.145.2, 200.201.145.63



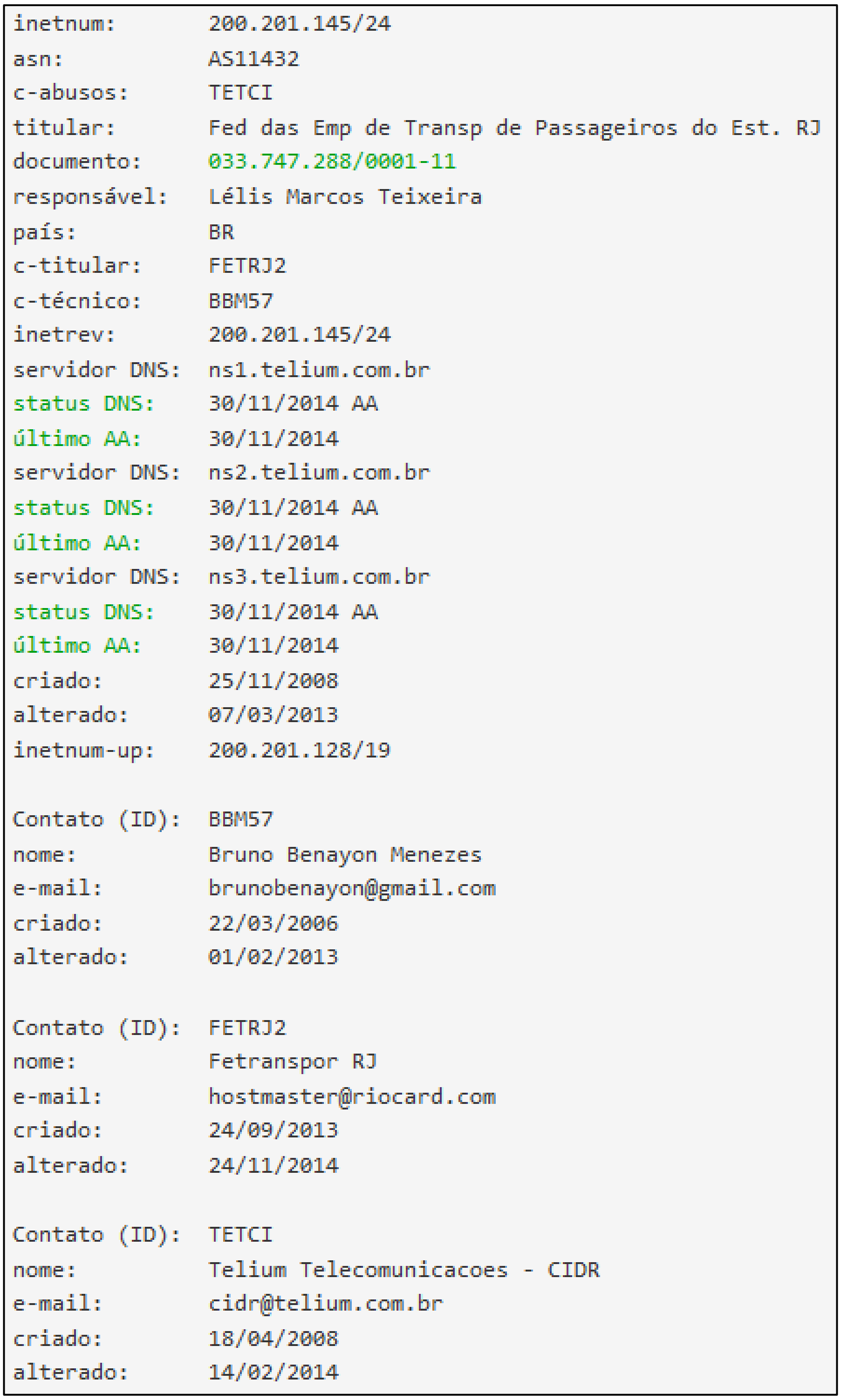
```
root@kali:~# whois 192.230.74.73

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# http://www.arin.net/public/whoisinaccuracy/index.xhtml
#


#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=192.230.74.73?showDetails=true&showARIN=false&ext=netref2
#

NetRange:       192.230.64.0 - 192.230.127.255
CIDR:           192.230.64.0/18
NetName:        INCAPSULA-NETWORK
NetHandle:      NET-192-230-64-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS19551
Organization:   Incapsula Inc (INCAP-5)
RegDate:        2013-05-08
Updated:        2013-05-08
Ref:            http://whois.arin.net/rest/net/NET-192-230-64-0-1

OrgName:        Incapsula Inc
OrgId:          INCAP-5
Address:        3500 SOUTH DUPONT HIGHWAY
City:           Dover
StateProv:      DE
PostalCode:     19901
Country:        US
RegDate:        2010-09-15
Updated:        2014-06-12
Ref:            http://whois.arin.net/rest/org/INCAP-5

OrgNOCHandle: INCAP2-ARIN
OrgNOCName:   Incapsula Operations
OrgNOCPhone:  +1-866-250-7659
OrgNOCEmail:  ip@incapsula.com
OrgNOCRef:    http://whois.arin.net/rest/poc/INCAP2-ARIN

OrgTechHandle: BRONS9-ARIN
OrgTechName:   Bronstein, Tomer
OrgTechPhone:  +1-866-250-7659
OrgTechEmail:  tomer@incapsula.com
OrgTechRef:    http://whois.arin.net/rest/poc/BRONS9-ARIN

OrgAbuseHandle: INCAP1-ARIN
```



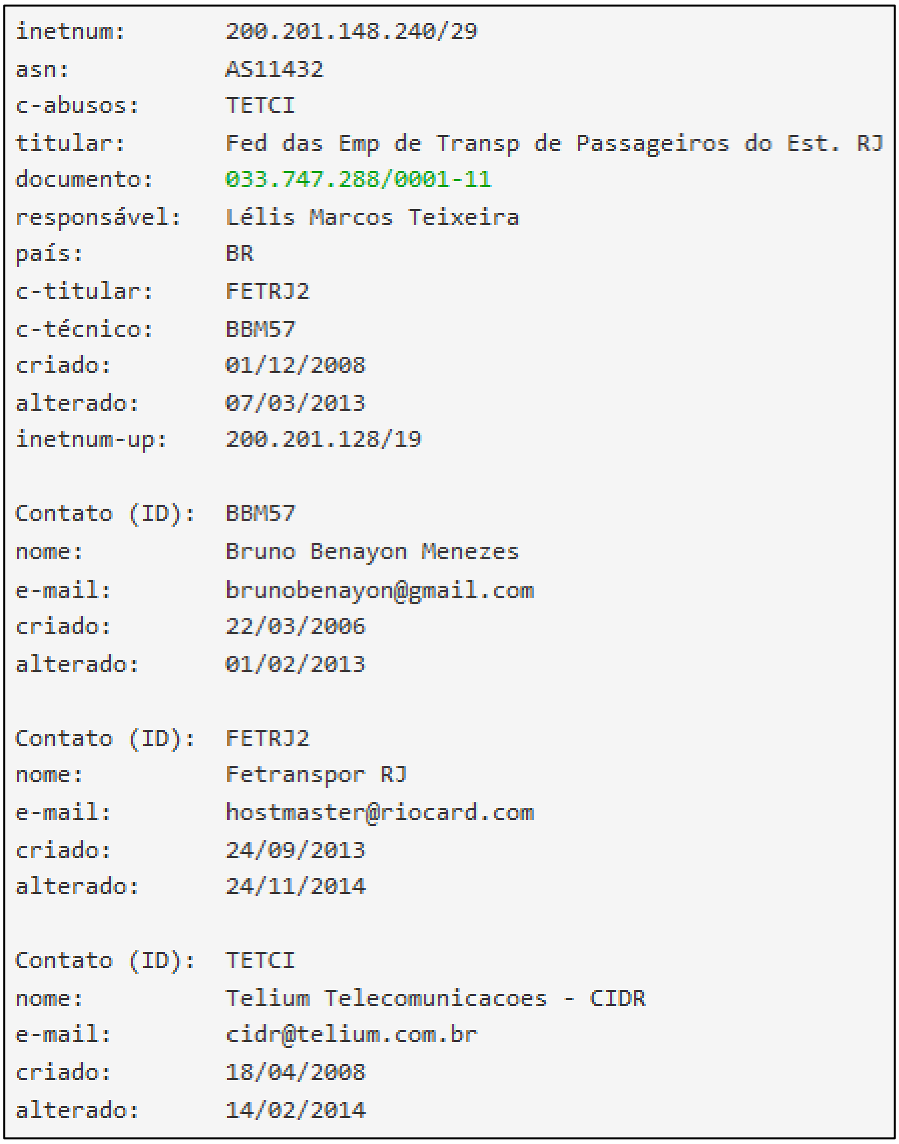
```
root@kali:~# whois 199.83.135.7

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# http://www.arin.net/public/whoisinaccuracy/index.xhtml
#



#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=199.83.135.7?showDetails=true&showARIN=false&ext=netref2
#

NetRange:       199.83.128.0 - 199.83.135.255
CIDR:           199.83.128.0/21
NetName:        INCAPSULA
NetHandle:      NET-199-83-128-0-1
Parent:         NET199 (NET-199-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS19551
Organization:   Incapsula Inc (INCAP-5)
RegDate:        2011-01-14
Updated:        2012-02-24
Ref:            http://whois.arin.net/rest/net/NET-199-83-128-0-1

OrgName:        Incapsula Inc
OrgId:          INCAP-5
Address:        3500 SOUTH DUPONT HIGHWAY
City:           Dover
StateProv:      DE
PostalCode:     19901
Country:        US
RegDate:        2010-09-15
Updated:        2014-06-12
Ref:            http://whois.arin.net/rest/org/INCAP-5

OrgAbuseHandle: INCAP1-ARIN
OrgAbuseName:   Incapsula AbuseDesk
OrgAbusePhone:  +1-866-250-7659
OrgAbuseEmail:  abuse@incapsula.com
OrgAbuseRef:    http://whois.arin.net/rest/poc/INCAP1-ARIN

OrgTechHandle: INCAP2-ARIN
OrgTechName:   Incapsula Operations
OrgTechPhone:  +1-866-250-7659
OrgTechEmail:  ip@incapsula.com
OrgTechRef:    http://whois.arin.net/rest/poc/INCAP2-ARIN

OrgTechHandle: BRONS9-ARIN
```



```
root@kali:~# whois 199.83.135.200

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# http://www.arin.net/public/whoisinaccuracy/index.xhtml
#


#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=199.83.135.200?showDetails=true&showARIN=false&ext=netref2
#

NetRange:       199.83.128.0 - 199.83.135.255
CIDR:           199.83.128.0/21
NetName:        INCAPSULA
NetHandle:      NET-199-83-128-0-1
Parent:         NET199 (NET-199-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS19551
Organization:   Incapsula Inc (INCAP-5)
RegDate:        2011-01-14
Updated:        2012-02-24
Ref:            http://whois.arin.net/rest/net/NET-199-83-128-0-1

OrgName:        Incapsula Inc
OrgId:          INCAP-5
Address:        3500 SOUTH DUPONT HIGHWAY
City:           Dover
StateProv:      DE
PostalCode:     19901
Country:        US
RegDate:        2010-09-15
Updated:        2014-06-12
Ref:            http://whois.arin.net/rest/org/INCAP-5

OrgTechHandle: BRONS9-ARIN
OrgTechName:   Bronstein, Tomer
OrgTechPhone:  +1-866-250-7659
OrgTechEmail:  tomer@incapsula.com
OrgTechRef:    http://whois.arin.net/rest/poc/BRONS9-ARIN

OrgAbuseHandle: INCAP1-ARIN
OrgAbuseName:   Incapsula AbuseDesk
OrgAbusePhone:  +1-866-250-7659
OrgAbuseEmail:  abuse@incapsula.com
OrgAbuseRef:    http://whois.arin.net/rest/poc/INCAP1-ARIN

OrgTechHandle: INCAP2-ARIN
```



```
inetnum:        200.201.145/24
asn:            AS11432
c-abusos:       TETCI
titular:        Fed das Emp de Transp de Passageiros do Est. RJ
documento:      033.747.288/0001-11
responsável:    Lélis Marcos Teixeira
país:           BR
c-titular:      FETRJ2
c-técnico:      BBM57
inetrev:        200.201.145/24
servidor DNS:   ns1.telium.com.br
status DNS:     30/11/2014 AA
último AA:      30/11/2014
servidor DNS:   ns2.telium.com.br
status DNS:     30/11/2014 AA
último AA:      30/11/2014
servidor DNS:   ns3.telium.com.br
status DNS:     30/11/2014 AA
último AA:      30/11/2014
criado:         25/11/2008
alterado:       07/03/2013
inetnum-up:     200.201.128/19

Contato (ID):   BBM57
nome:           Bruno Benayon Menezes
e-mail:         brunobenayon@gmail.com
criado:         22/03/2006
alterado:       01/02/2013

Contato (ID):   FETRJ2
nome:           Fetranspor RJ
e-mail:         hostmaster@riocard.com
criado:         24/09/2013
alterado:       24/11/2014

Contato (ID):   TETCI
nome:           Telium Telecomunicacoes - CIDR
e-mail:         cidr@telium.com.br
criado:         18/04/2008
alterado:       14/02/2014
```



```
inetnum:       200.201.148.240/29
asn:           AS11432
c-abusos:      TETCI
titular:       Fed das Emp de Transp de Passageiros do Est. RJ
documento:     033.747.288/0001-11
responsável:   Lélis Marcos Teixeira
país:          BR
c-titular:     FETRJ2
c-técnico:     BBM57
criado:        01/12/2008
alterado:      07/03/2013
inetnum-up:    200.201.128/19

Contato (ID):  BBM57
nome:          Bruno Benayon Menezes
e-mail:        brunobenayon@gmail.com
criado:        22/03/2006
alterado:      01/02/2013

Contato (ID):  FETRJ2
nome:          Fetranspor RJ
e-mail:        hostmaster@riocard.com
criado:        24/09/2013
alterado:      24/11/2014

Contato (ID):  TETCI
nome:          Telium Telecomunicacoes - CIDR
e-mail:        cidr@telium.com.br
criado:        18/04/2008
alterado:      14/02/2014
```

Resultados Obtidos: Foi possível identificar informações sobre contatos, responsáveis pelos endereços, CNPJ, servidores DNS.

Descrição: Informações sobre contatos e endereços de email com domínio não corporativo puderam ser identificadas através de consultas em serviços gratuitos publicados na internet (registro.br).

Impacto: Obtenção de informações pessoais que podem ser utilizadas para futuros ataques.

Severidade: Baixa

Recomendação: É recomendado que nenhuma informação particular de funcionários ou prestadores de serviços sejam expostos publicamente na internet. Verificar a possibilidade de inserir um endereço de email genérico com domínio corporativo, por exemplo segurança@riocard.com. (ANEXO B)

4.1.3. Análise e Validação das vulnerabilidades

4.1.3.1. Teste de invasão externo de aplicação web

O teste de invasão externo de aplicação *web* foi conduzido em dois tipos de testes: (a) varreduras automatizada; e (b) validações manuais de vulnerabilidades.

Adicionalmente, também foram evidenciadas as validações manuais de vulnerabilidades sem sucesso.

Durante os testes, foi identificada a existência de controles de segurança, como: (a) presença de *firewall* de aplicação (WAF); e (b) bloqueios de requisições maliciosas.

A existência desses controles de segurança dificultam as ações do atacante, principalmente a presença do *WAF* (Firewall de aplicação) que, após sucessivas requisições maliciosas, realiza o bloqueio do endereço IP do atacante, impossibilitando-o ter acesso ao site a partir do seu endereço IP.

A fase de varredura automática realiza diversas verificações em busca de vulnerabilidades conhecidas. Além da varredura automática, também foram realizados testes manuais em busca de possíveis vulnerabilidades.

(a) Varredura Automatizada

Para a fase de varredura automatizada, foi utilizada a ferramenta *Acunetix*, que realiza requisições para verificação de diversas vulnerabilidades conhecidas.

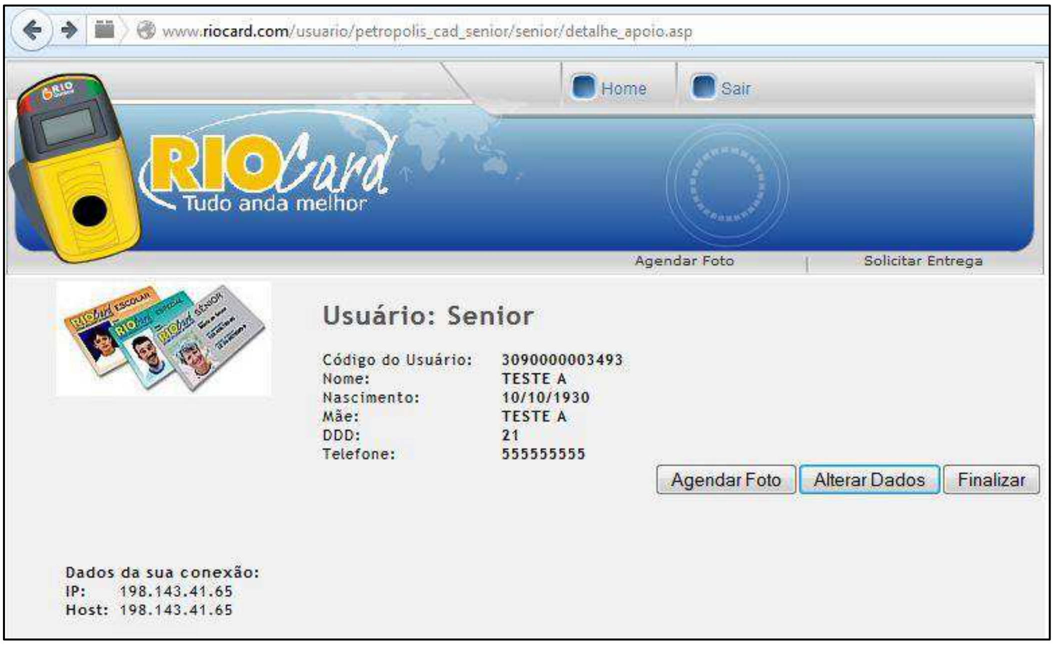
Com base no escopo do Termo de Referência, os seguintes testes foram cobertos na varredura automatizada:

Teste	***Descrição***
1) SQL *Injection*	Verificar a possibilidade de inserção de dados nos aplicativos que executam consultas SQL.
2) Code Injection	Verificar a possibilidade de injetar dados nos aplicativos para serem executados posteriormente pelo servidor web.
3) Manipulação de URLs	Verificar se há possibilidade de um agente mal-intencionado manipular certas partes das URLs, levando um servidor *web* a emitir páginas às quais não é suposto ter acesso.
4) Validação de dados	Testar possíveis formas de entrada, para entender se a aplicação valida

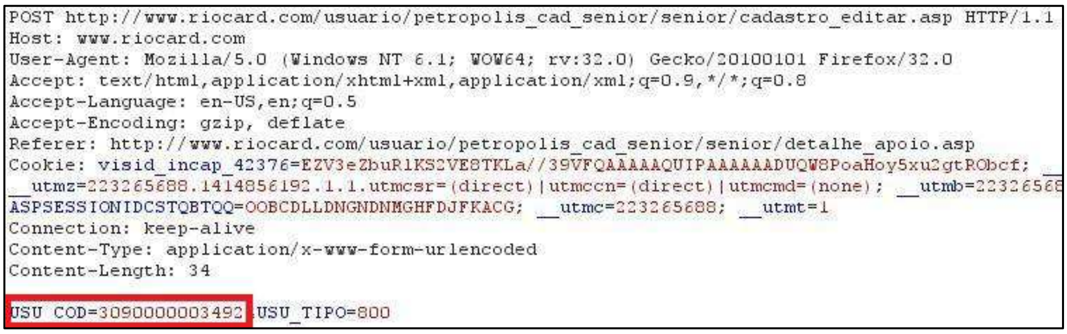
Teste	***Descrição***
	suficientemente os dados de entrada antes de utilizá-los. *
5) Escalação privilégios	Verificar a possibilidade de um usuário modificar seus privilégios e/ou funções dentro do aplicativo de modo a permitir ataques.
6) Obtenção de informações por *sniffer*	Obter informações através da interceptação dos dados trafegados na rede.
7) Vulnerabilidades de AJAX (Asynchronous Javascript and XML)	Verificar se a aplicação possui um nível de proteção adequado para as vulnerabilidades inerentes ao uso do modelo AJAX, tais como: aumento da superfície de ataque, exposição de funções internas da aplicação, acesso indevido a recursos de terceiros com proteção inadequada, falha na proteção de autenticação de informações e sessões, entre outros.
8) Inclusão de arquivos	Verificar se as aplicações permitem que um usuário não autenticado consiga realizar *upload* de arquivos para o servidor *web* ou até mesmo substituir outros arquivos a fim de comprometer as aplicações.
9) Manipulação de *cookies*	Verificar se as aplicações possuem proteções adequadas para os *cookies*, testando se estas proteções foram configuradas corretamente a fim de evitar ataques.
10) Manipulação de campos de dados	Verificar se as aplicações possuem proteções adequadas para evitar a manipulação indevida de campos de dados, testando se estas proteções foram configuradas corretamente.
11) Utilização de informações em mensagens de erro	Informações como códigos de erro podem informar um usuário malicioso sobre tecnologias e produtos que estão sendo usados pelo aplicativo. Muitas vezes, esse código de erro fornece informações potencialmente úteis a um atacante.
12) Uso de sessão de terceiros	Verificar se os *cookies* e outros *tokens* de sessões são criados de forma segura e imprevisível a fim de evitar que um atacante consiga roubar sessões de usuários legítimos e se passar por eles.
13) Quebra de criptografia	Verificar se os dados de autenticação do usuário são transferidos através de um canal criptografado para evitar ser interceptado por usuários mal-intencionados.
14) XSS (*Cross-Site Scripting*)	Verificar se as aplicações *web* permitem que um usuário malicioso injete códigos *Javascript* maliciosos que são executados pelos navegadores dos clientes a fim de realizar ataques.

(b) Validações Manuais de Vulnerabilidades

As tabelas abaixo exibem a realização de validações manuais de vulnerabilidades, tanto para as vulnerabilidades encontradas durante a varredura automatizada, quanto para validações manuais de possíveis vulnerabilidades.

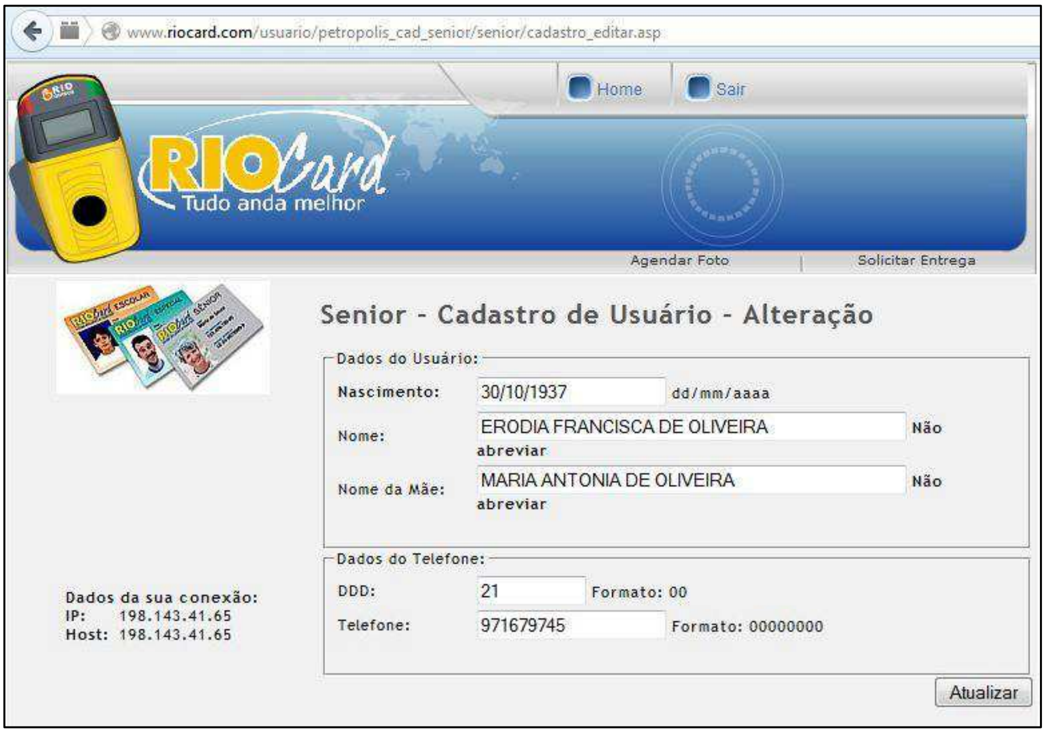
#1	***Failure to Restrict URL Access***
Descrição da Vulnerabilidade Por meio dos testes manuais verificamos problemas no controle de sessão e no controle de restrição a URLs dos sites analisados.	
URLs Afetados	http://www.riocard.com/
Impacto	Por meio das páginas acessíveis pela listagem de diretório, foi possível realizar a criação de um usuário fictício "TESTE A".
Severidade	Crítica
Evidência	*Por meio das páginas acessíveis pela listagem de diretório, foi possível realizar a criação de um usuário fictício "TESTE A". Com a geração de um código para esse usuário: "3090000003493".*  www.riocard.com/usuario/petropolis_cad_senior/senior/detalhe_apoio.asp Usuário: Senior Código do Usuário: 3090000003493 Nome: TESTE A Nascimento: 10/10/1930 Mãe: TESTE A DDD: 21 Telefone: 555555555 Dados da sua conexão: IP: 198.143.41.65 Host: 198.143.41.65 Home Sair RIOCard Tudo anda melhor Agendar Foto Solicitar Entrega Agendar Foto Alterar Dados Finalizar *Com isso, foi selecionado o botão "Alterar Dados" para alterar os dados cadastrais. Após isso, o tráfego foi interceptado pela ferramenta "Burp Suite", e o valor do campo "USU_COD" foi alterado para outro código, nesse caso o "3090000003492".*

#1 *Failure to Restrict URL Access*



```
POST http://www.riocard.com/usuario/petropolis_cad_senior/senior/cadastro_editar.asp HTTP/1.1
Host: www.riocard.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.riocard.com/usuario/petropolis_cad_senior/senior/detalhe_apoio.asp
Cookie: visid_incap_42376=EZV3eZbuR1KS2VE8TKLa//39VFQAAAAAQUIPAAAAAADUQW8PoaHoy5xu2gtRObcf; __
__utmz=223265688.1414856192.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); __utmb=2232656
ASPSESSIONIDCSTQBTQQ=OOBCDLLDNGNDNMGHFDJFKACG; __utmc=223265688; __utmt=1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 34

USU COD=3090000003492 USU_TIPO=800
```

Depois de realizada essa alteração, foi possível acessar uma área para alteração de dados, porém com os dados de outra pessoa (com o código "3090000003492").



www.riocard.com/usuario/petropolis_cad_senior/senior/cadastro_editar.asp
Home
Sair
RIOCard
Tudo anda melhor
Agendar Foto
Solicitar Entrega

Senior - Cadastro de Usuário - Alteração

Dados do Usuário:

Nascimento: 30/10/1937 dd/mm/aaaa

Nome: ERODIA FRANCISCA DE OLIVEIRA Não abreviar

Nome da Mãe: MARIA ANTONIA DE OLIVEIRA Não abreviar

Dados do Telefone:

DDD: 21 Formato: 00

Telefone: 971679745 Formato: 00000000

Dados da sua conexão:
IP: 198.143.41.65
Host: 198.143.41.65

Observação: Nenhum dado de usuários foi alterado durante os testes.

Recomendação	É recomendável que se use restrição de permissão para que visitantes visualizem e alterem informações restritas.
Data do Teste	04/11/2014

#1	***Failure to Restrict URL Access***
Tipo de Teste Executado	Manipulação de URLs

#2	***Cleartext submission of password***

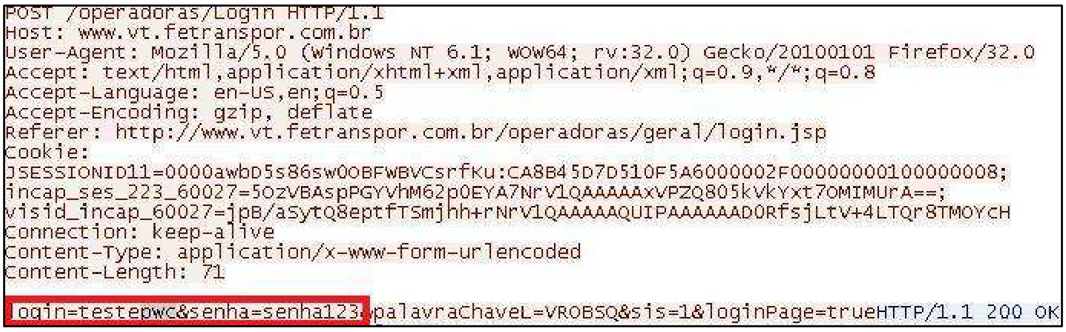
Descrição da Vulnerabilidade

Senhas estão sendo transmitidas por um canal não criptografado. Um usuário malicioso pode interceptar as senhas por esse canal.

Este tipo de informação deve ser transferido sempre por canais criptografados (HTTPS) para evitar a interceptação das informações por usuários maliciosos.

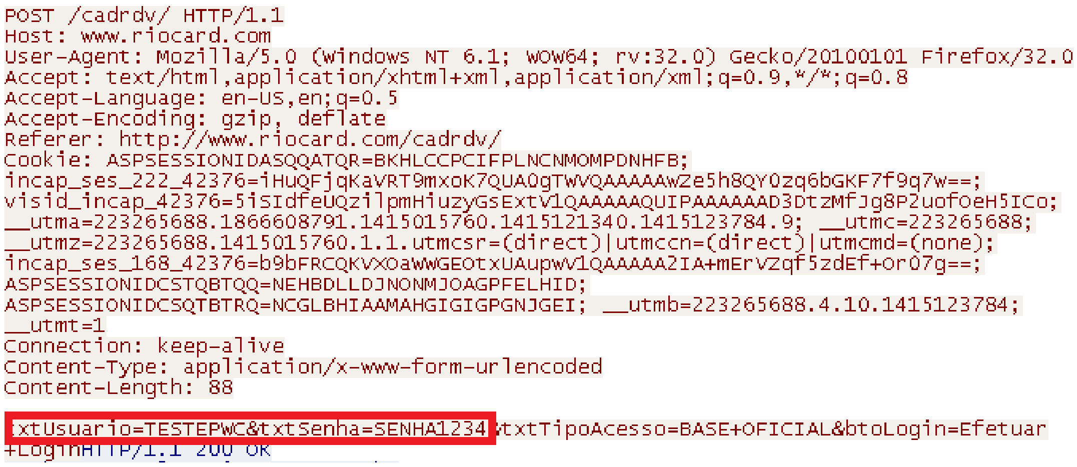
URLs Afetados	http://www.vt.fetranspor.com.br/operadoras/ http://www.riocard.com
Impacto	É possível que informações sensíveis como login e senha de usuários sejam capturadas.
Severidade	Alto

Evidência



```
POST /operadoras/Login HTTP/1.1
Host: www.vt.fetranspor.com.br
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.vt.fetranspor.com.br/operadoras/geral/login.jsp
Cookie:
JSESSIONID11=0000awbD5s86sw0OBFWBVCsrfKu:CA8B45D7D510F5A6000002F000000000100000008;
incap_ses_223_60027=5OzVBAspPGYVhM62p0EYA7NrV1QAAAAAxVPZQ805kVkYxt7OMIMUrA==;
visid_incap_60027=jpB/aSytQ8eptfTSmjhh+rNrV1QAAAAAQUIPAAAAAAD0RfsjLtV+4LTQr8TMOYcH
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 71

login=testepwc&senha=senha123&palavraChaveL=VROBSQ&sis=1&loginPage=trueHTTP/1.1 200 OK
```

#2	***Cleartext submission of password***



```
POST /cadrdv/ HTTP/1.1
Host: www.riocard.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.riocard.com/cadrdv/
Cookie: ASPSESSIONIDASQQATQR=BKHLCCPCIFPLNCNMOMPDNHFB;
incap_ses_222_42376=iHuQFjqKaVRT9mxoK7QUA0gTWVQAAAAAwZe5h8QY0zq6bGKF7f9q7w==;
visid_incap_42376=5isIdfeUQzilpmHiuzyGsExtV1QAAAAAQUIPAAAAAAAD3DtzMfJg8P2uofoeH5ICo;
__utma=223265688.1866608791.1415015760.1415121340.1415123784.9; __utmc=223265688;
__utmz=223265688.1415015760.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
incap_ses_168_42376=b9bFRCQKVXOaWWGEOtxUAupwV1QAAAAA2IA+mErVZqf5zdEf+Or07g==;
ASPSESSIONIDCSTQBTQQ=NEHBDLLDJNONMJOAGPFELHID;
ASPSESSIONIDCSQTBTRQ=NCGLBHIAAMAHGIGIGPGNJGEI; __utmb=223265688.4.10.1415123784;
__utmt=1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 88

xtUsuario=TESTEPWC&txtSenha=SENHA1234 txtTipoAcesso=BASE+OFICIAL&btoLogin=Efetuar
+LoginHTTP/1.1 200 OK
```

Recomendação	É recomendável que as informações sensíveis sejam trafegadas por conexões criptografadas (HTTPS) para que os dados não sejam interceptados por um usuário malicioso.
Data do Teste	03/11/2014
Tipo de Teste Executado	Obtenção de informações - *sniffer*

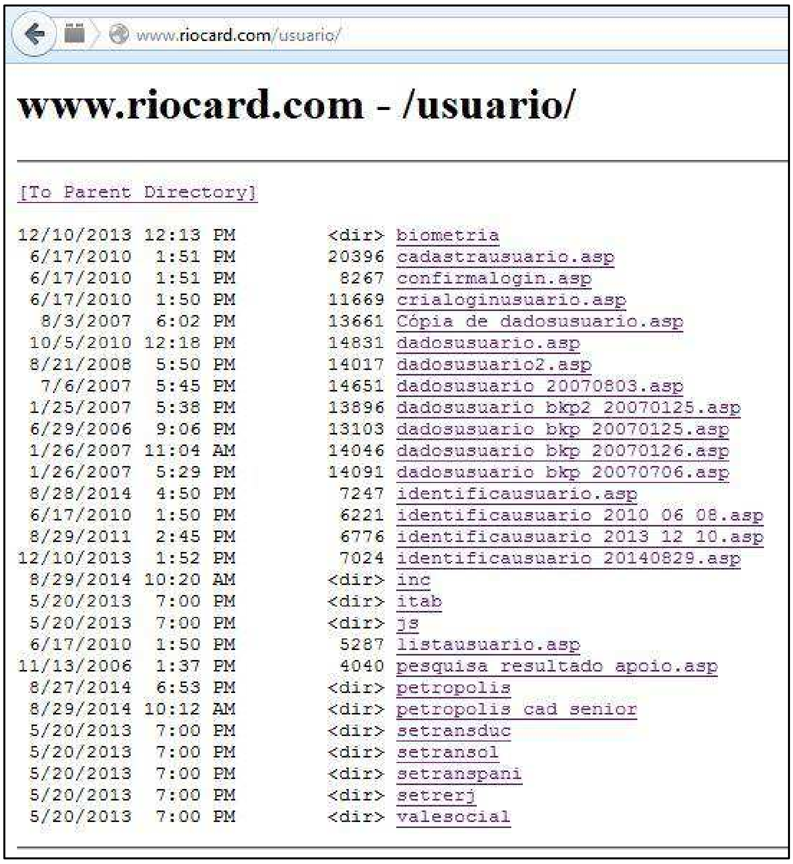
#3 *Directory Listing*

Descrição da Vulnerabilidade

O Web Server se encontra configurado para mostrar a lista de arquivos contidos em seus diretórios, dentre esses arquivos podem estar contidos diversas informações que podem ser confidenciais ou podem ser utilizadas para gerar um ataque mais sofisticado a esse servidor.

URLs Afetados	http://www.riocard.com/images http://www.riocard.com/noticias http://www.riocard.com/Scripts http://www.riocard.com/style http://www.riocard.com/swf http://www.riocard.com/usuario http://www.riocard.com/cadrdv
Impacto	Por meio dessa vulnerabilidade foi possível ter acesso a diversas páginas do site e, com isso, obter informações sensíveis de usuários.
Severidade	Médio

Evidência



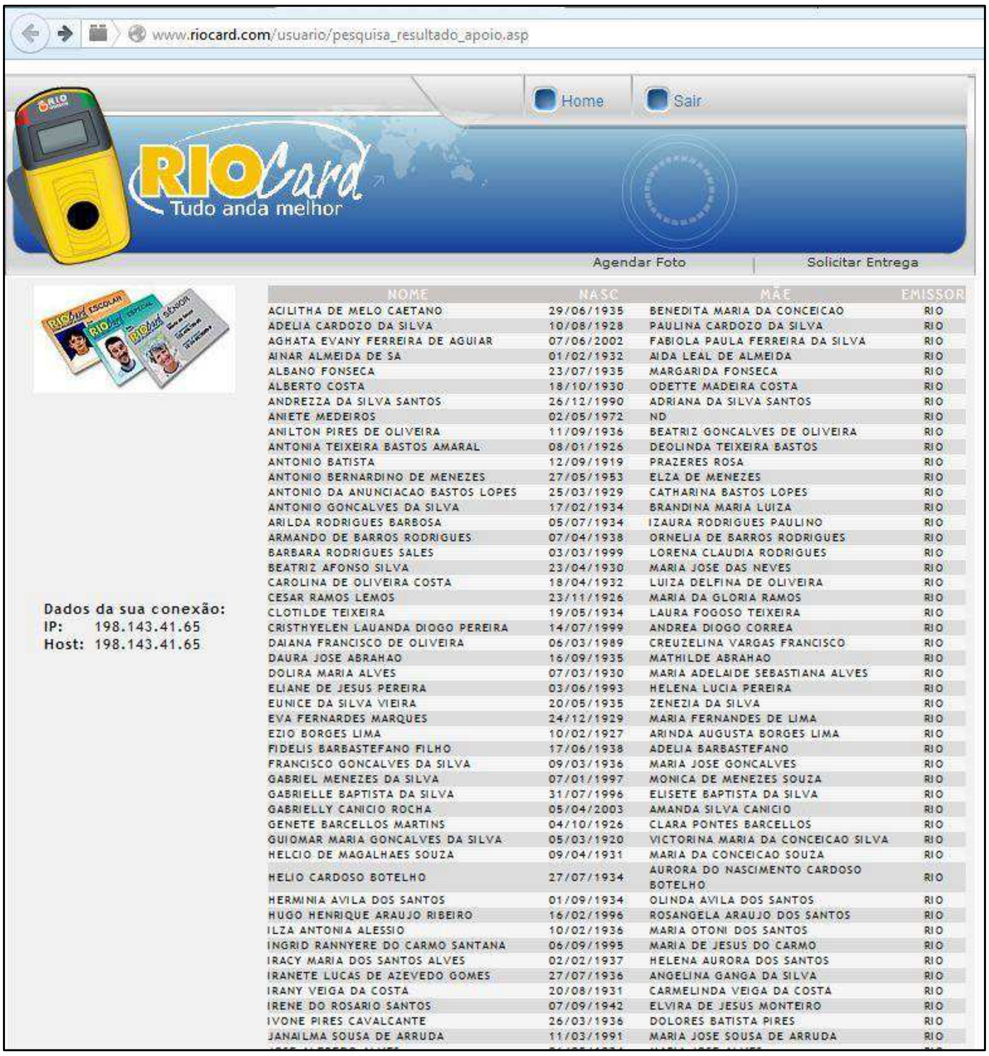
```
www.riocard.com - /usuario/

[To Parent Directory]

12/10/2013 12:13 PM        <dir> biometria
 6/17/2010  1:51 PM        20396 cadastrausuario.asp
 6/17/2010  1:51 PM         8267 confirmalogin.asp
 6/17/2010  1:50 PM        11669 crialoginusuario.asp
  8/3/2007  6:02 PM        13661 Cópia de dadosusuario.asp
 10/5/2010 12:18 PM        14831 dadosusuario.asp
 8/21/2008  5:50 PM        14017 dadosusuario2.asp
  7/6/2007  5:45 PM        14651 dadosusuario 20070803.asp
 1/25/2007  5:38 PM        13896 dadosusuario bkp2 20070125.asp
 6/29/2006  9:06 PM        13103 dadosusuario bkp 20070125.asp
 1/26/2007 11:04 AM        14046 dadosusuario bkp 20070126.asp
 1/26/2007  5:29 PM        14091 dadosusuario bkp 20070706.asp
 8/28/2014  4:50 PM         7247 identificausuario.asp
 6/17/2010  1:50 PM         6221 identificausuario 2010 06 08.asp
 8/29/2011  2:45 PM         6776 identificausuario 2013 12 10.asp
12/10/2013  1:52 PM         7024 identificausuario 20140829.asp
 8/29/2014 10:20 AM        <dir> inc
 5/20/2013  7:00 PM        <dir> itab
 5/20/2013  7:00 PM        <dir> js
 6/17/2010  1:50 PM         5287 listausuario.asp
11/13/2006  1:37 PM         4040 pesquisa resultado apoio.asp
 8/27/2014  6:53 PM        <dir> petropolis
 8/29/2014 10:12 AM        <dir> petropolis cad senior
 5/20/2013  7:00 PM        <dir> setransduc
 5/20/2013  7:00 PM        <dir> setransol
 5/20/2013  7:00 PM        <dir> setranspani
 5/20/2013  7:00 PM        <dir> setrerj
 5/20/2013  7:00 PM        <dir> valesocial
```

Por meio desta vulnerabilidade, foi possível acessar as páginas disponíveis dentro dessa

#3 ***Directory Listing***

listagem de diretórios. A imagem 1 abaixo mostra uma página acessada que consta uma lista de usuários do sistema.

Imagem 1



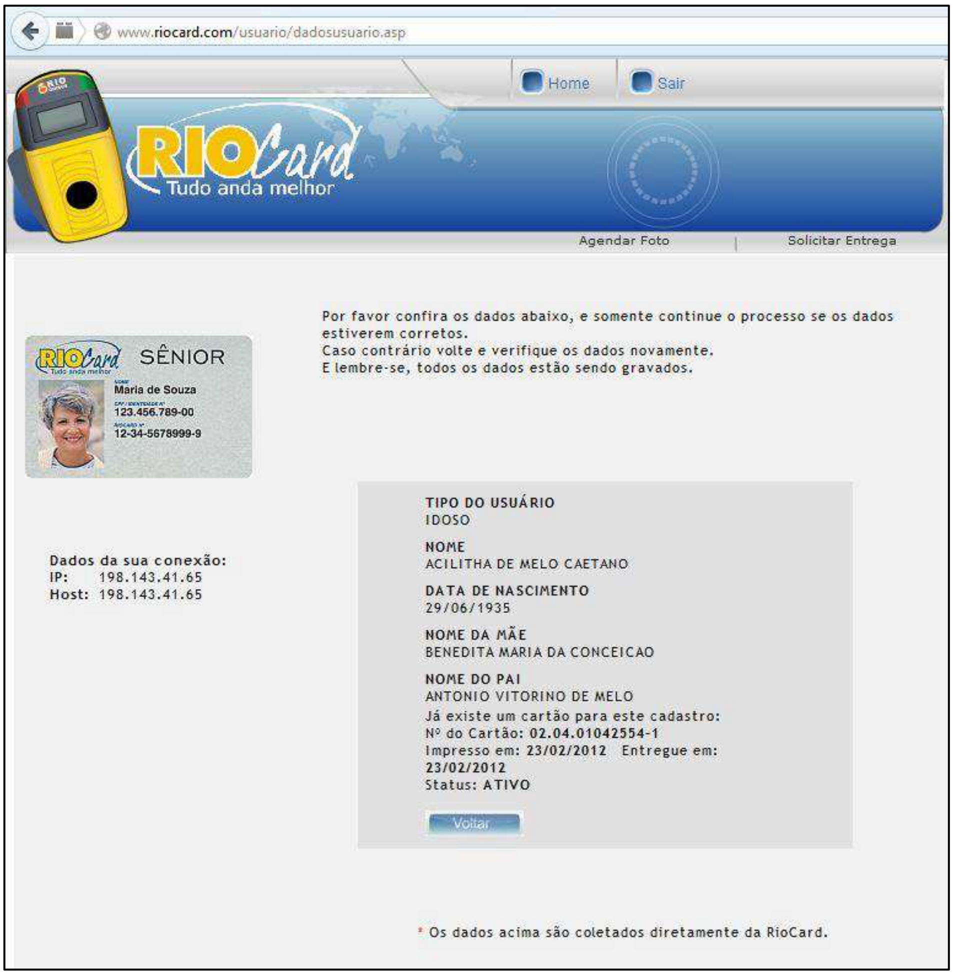
Dados da sua conexão:
IP: 198.143.41.65
Host: 198.143.41.65

NOME	NASC	MÃE	EMISSOR
ACILITHA DE MELO CAETANO	29/06/1935	BENEDITA MARIA DA CONCEICAO	RIO
ADELIA CARDOZO DA SILVA	10/08/1928	PAULINA CARDOZO DA SILVA	RIO
AGHATA EVANY FERREIRA DE AGUIAR	07/06/2002	FABIOLA PAULA FERREIRA DA SILVA	RIO
AINAR ALMEIDA DE SA	01/02/1932	AIDA LEAL DE ALMEIDA	RIO
ALBANO FONSECA	23/07/1935	MARGARIDA FONSECA	RIO
ALBERTO COSTA	18/10/1930	ODETTE MADEIRA COSTA	RIO
ANDREZZA DA SILVA SANTOS	26/12/1990	ADRIANA DA SILVA SANTOS	RIO
ANIETE MEDEIROS	02/05/1972	ND	RIO
ANILTON PIRES DE OLIVEIRA	11/09/1936	BEATRIZ GONCALVES DE OLIVEIRA	RIO
ANTONIA TEIXEIRA BASTOS AMARAL	08/01/1926	DEOLINDA TEIXEIRA BASTOS	RIO
ANTONIO BATISTA	12/09/1919	PRAZERES ROSA	RIO
ANTONIO BERNARDINO DE MENEZES	27/05/1953	ELZA DE MENEZES	RIO
ANTONIO DA ANUNCIACAO BASTOS LOPES	25/03/1929	CATHARINA BASTOS LOPES	RIO
ANTONIO GONCALVES DA SILVA	17/02/1934	BRANDINA MARIA LUIZA	RIO
ARILDA RODRIGUES BARBOSA	05/07/1934	IZAURA RODRIGUES PAULINO	RIO
ARMANDO DE BARROS RODRIGUES	07/04/1938	ORNELIA DE BARROS RODRIGUES	RIO
BARBARA RODRIGUES SALES	03/03/1999	LORENA CLAUDIA RODRIGUES	RIO
BEATRIZ AFONSO SILVA	23/04/1930	MARIA JOSE DAS NEVES	RIO
CAROLINA DE OLIVEIRA COSTA	18/04/1932	LUIZA DELFINA DE OLIVEIRA	RIO
CESAR RAMOS LEMOS	23/11/1926	MARIA DA GLORIA RAMOS	RIO
CLOTILDE TEIXEIRA	19/05/1934	LAURA FOGOSO TEIXEIRA	RIO
CRISTHYELEN LAUANDA DIOGO PEREIRA	14/07/1999	ANDREA DIOGO CORREA	RIO
DAIANA FRANCISCO DE OLIVEIRA	06/03/1989	CREUZELINA VARGAS FRANCISCO	RIO
DAURA JOSE ABRAHAO	16/09/1935	MATHILDE ABRAHAO	RIO
DOLIRA MARIA ALVES	07/03/1930	MARIA ADELAIDE SEBASTIANA ALVES	RIO
ELIANE DE JESUS PEREIRA	03/06/1993	HELENA LUCIA PEREIRA	RIO
EUNICE DA SILVA VIEIRA	20/05/1935	ZENEZIA DA SILVA	RIO
EVA FERNARDES MARQUES	24/12/1929	MARIA FERNANDES DE LIMA	RIO
EZIO BORGES LIMA	10/02/1927	ARINDA AUGUSTA BORGES LIMA	RIO
FIDELIS BARBASTEFANO FILHO	17/06/1938	ADELIA BARBASTEFANO	RIO
FRANCISCO GONCALVES DA SILVA	09/03/1936	MARIA JOSE GONCALVES	RIO
GABRIEL MENEZES DA SILVA	07/01/1997	MONICA DE MENEZES SOUZA	RIO
GABRIELLE BAPTISTA DA SILVA	31/07/1996	ELISETE BAPTISTA DA SILVA	RIO
GABRIELLY CANICIO ROCHA	05/04/2003	AMANDA SILVA CANICIO	RIO
GENETE BARCELLOS MARTINS	04/10/1926	CLARA PONTES BARCELLOS	RIO
GUIOMAR MARIA GONCALVES DA SILVA	05/03/1920	VICTORINA MARIA DA CONCEICAO SILVA	RIO
HELCIO DE MAGALHAES SOUZA	09/04/1931	MARIA DA CONCEICAO SOUZA	RIO
HELIO CARDOSO BOTELHO	27/07/1934	AURORA DO NASCIMENTO CARDOSO BOTELHO	RIO
HERMINIA AVILA DOS SANTOS	01/09/1934	OLINDA AVILA DOS SANTOS	RIO
HUGO HENRIQUE ARAUJO RIBEIRO	16/02/1996	ROSANGELA ARAUJO DOS SANTOS	RIO
ILZA ANTONIA ALESSIO	10/02/1936	MARIA OTONI DOS SANTOS	RIO
INGRID RANNYERE DO CARMO SANTANA	06/09/1995	MARIA DE JESUS DO CARMO	RIO
IRACY MARIA DOS SANTOS ALVES	02/02/1937	HELENA AURORA DOS SANTOS	RIO
IRANETE LUCAS DE AZEVEDO GOMES	27/07/1936	ANGELINA GANGA DA SILVA	RIO
IRANY VEIGA DA COSTA	20/08/1931	CARMELINDA VEIGA DA COSTA	RIO
IRENE DO ROSARIO SANTOS	07/09/1942	ELVIRA DE JESUS MONTEIRO	RIO
IVONE PIRES CAVALCANTE	26/03/1936	DOLORES BATISTA PIRES	RIO
JANAILMA SOUSA DE ARRUDA	11/03/1991	MARIA JOSE SOUSA DE ARRUDA	RIO

#3 Directory Listing

A partir dessa lista, podemos selecionar um usuário para obter mais informações sobre ele, como mostra a imagem 2 abaixo.

Imagem 2


www.riocard.com/usuario/dadosusuario.asp
Home
Sair
RIOCard
Tudo anda melhor
Agendar Foto
Solicitar Entrega
RIOCard SÊNIOR
Maria de Souza
123.456.789-00
12-34-5678999-9
Voltar

Por favor confira os dados abaixo, e somente continue o processo se os dados estiverem corretos.
Caso contrário volte e verifique os dados novamente.
E lembre-se, todos os dados estão sendo gravados.

Dados da sua conexão:
IP: 198.143.41.65
Host: 198.143.41.65

TIPO DO USUÁRIO
IDOSO

NOME
ACILITHA DE MELO CAETANO

DATA DE NASCIMENTO
29/06/1935

NOME DA MÃE
BENEDITA MARIA DA CONCEICAO

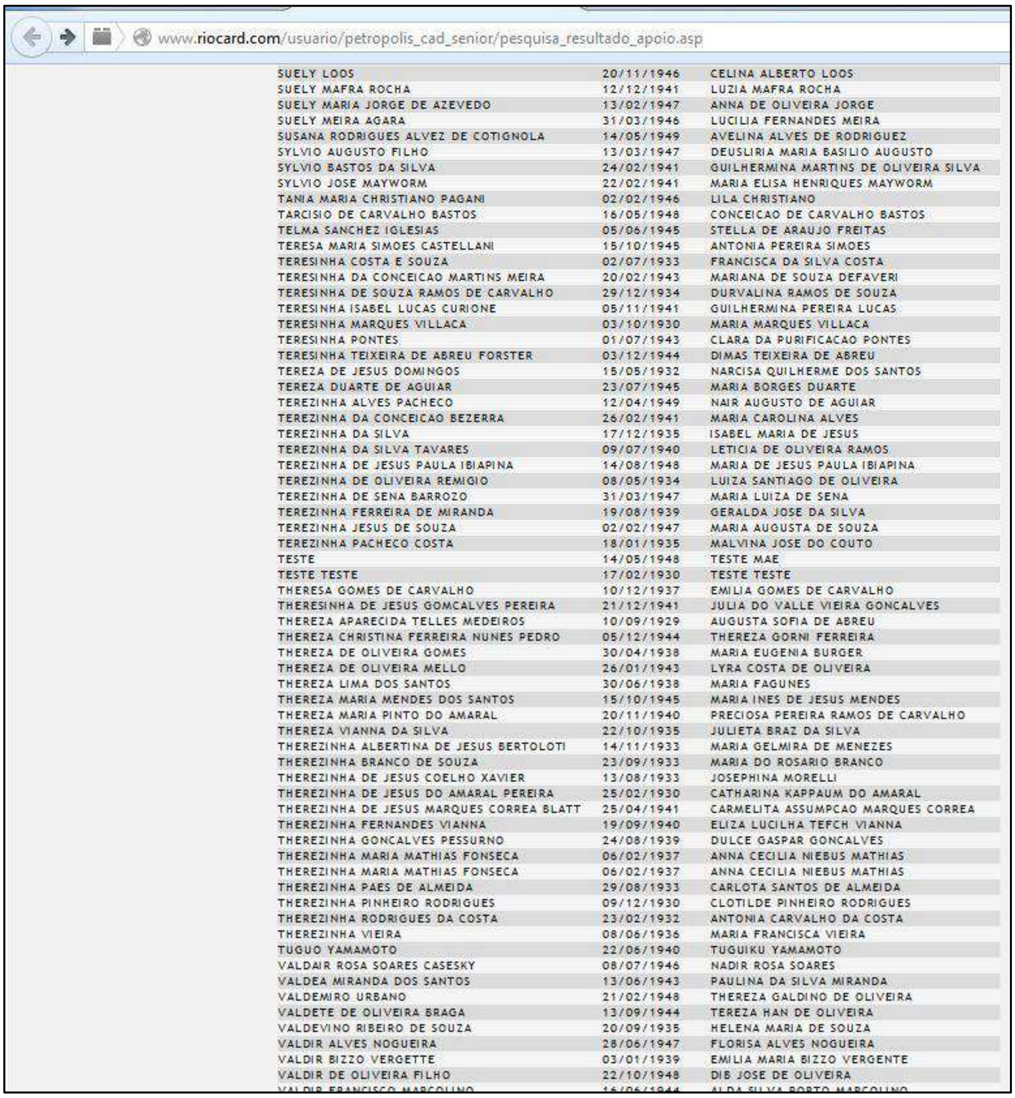
NOME DO PAI
ANTONIO VITORINO DE MELO
Já existe um cartão para este cadastro:
Nº do Cartão: **02.04.01042554-1**
Impresso em: **23/02/2012** Entregue em: **23/02/2012**
Status: **ATIVO**

* Os dados acima são coletados diretamente da RioCard.

#3 *Directory Listing*

Durante a verificação de algumas páginas disponíveis nessa listagem de diretórios, conseguimos visualizar alguns usuários com o nome “TESTE” (vide imagem 3).

Imagem 3



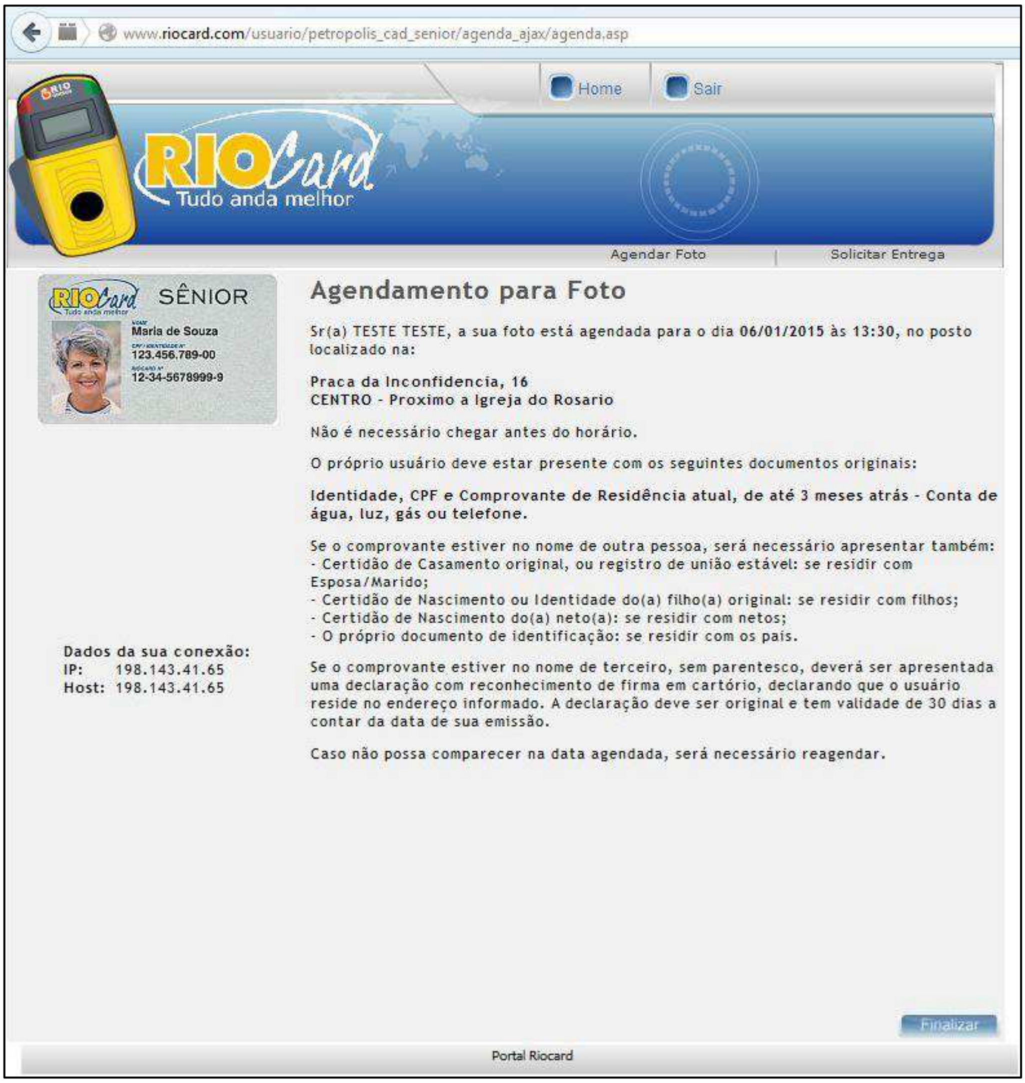
www.riocard.com/usuario/petropolis_cad_senior/pesquisa_resultado_apoio.asp

SUELY LOOS	20/11/1946	CELINA ALBERTO LOOS
SUELY MAFRA ROCHA	12/12/1941	LUZIA MAFRA ROCHA
SUELY MARIA JORGE DE AZEVEDO	13/02/1947	ANNA DE OLIVEIRA JORGE
SUELY MEIRA AGARA	31/03/1946	LUCILIA FERNANDES MEIRA
SUSANA RODRIGUES ALVEZ DE COTIGNOLA	14/05/1949	AVELINA ALVES DE RODRIGUEZ
SYLVIO AUGUSTO FILHO	13/03/1947	DEUSLIRIA MARIA BASILIO AUGUSTO
SYLVIO BASTOS DA SILVA	24/02/1941	GUILHERMINA MARTINS DE OLIVEIRA SILVA
SYLVIO JOSE MAYWORM	22/02/1941	MARIA ELISA HENRIQUES MAYWORM
TANIA MARIA CHRISTIANO PAGANI	02/02/1946	LILA CHRISTIANO
TARCISIO DE CARVALHO BASTOS	16/05/1948	CONCEICAO DE CARVALHO BASTOS
TELMA SANCHEZ IGLESIAS	05/06/1945	STELLA DE ARAUJO FREITAS
TERESA MARIA SIMOES CASTELLANI	15/10/1945	ANTONIA PEREIRA SIMOES
TERESINHA COSTA E SOUZA	02/07/1933	FRANCISCA DA SILVA COSTA
TERESINHA DA CONCEICAO MARTINS MEIRA	20/02/1943	MARIANA DE SOUZA DEFAVERI
TERESINHA DE SOUZA RAMOS DE CARVALHO	29/12/1934	DURVALINA RAMOS DE SOUZA
TERESINHA ISABEL LUCAS CURIONE	05/11/1941	GUILHERMINA PEREIRA LUCAS
TERESINHA MARQUES VILLACA	03/10/1930	MARIA MARQUES VILLACA
TERESINHA PONTES	01/07/1943	CLARA DA PURIFICACAO PONTES
TERESINHA TEIXEIRA DE ABREU FORSTER	03/12/1944	DIMAS TEIXEIRA DE ABREU
TEREZA DE JESUS DOMINGOS	15/05/1932	NARCISA QUILHERME DOS SANTOS
TEREZA DUARTE DE AGUIAR	23/07/1945	MARIA BORGES DUARTE
TEREZINHA ALVES PACHECO	12/04/1949	NAIR AUGUSTO DE AGUIAR
TEREZINHA DA CONCEICAO BEZERRA	26/02/1941	MARIA CAROLINA ALVES
TEREZINHA DA SILVA	17/12/1935	ISABEL MARIA DE JESUS
TEREZINHA DA SILVA TAVARES	09/07/1940	LETICIA DE OLIVEIRA RAMOS
TEREZINHA DE JESUS PAULA IBIAPINA	14/08/1948	MARIA DE JESUS PAULA IBIAPINA
TEREZINHA DE OLIVEIRA REMIGIO	08/05/1934	LUIZA SANTIAGO DE OLIVEIRA
TEREZINHA DE SENA BARROZO	31/03/1947	MARIA LUIZA DE SENA
TEREZINHA FERREIRA DE MIRANDA	19/08/1939	GERALDA JOSE DA SILVA
TEREZINHA JESUS DE SOUZA	02/02/1947	MARIA AUGUSTA DE SOUZA
TEREZINHA PACHECO COSTA	18/01/1935	MALVINA JOSE DO COUTO
TESTE	14/05/1948	TESTE MAE
TESTE TESTE	17/02/1930	TESTE TESTE
THERESA GOMES DE CARVALHO	10/12/1937	EMILIA GOMES DE CARVALHO
THERESINHA DE JESUS GOMCALVES PEREIRA	21/12/1941	JULIA DO VALLE VIEIRA GONCALVES
THEREZA APARECIDA TELLES MEDEIROS	10/09/1929	AUGUSTA SOFIA DE ABREU
THEREZA CHRISTINA FERREIRA NUNES PEDRO	05/12/1944	THEREZA GORNI FERREIRA
THEREZA DE OLIVEIRA GOMES	30/04/1938	MARIA EUGENIA BURGER
THEREZA DE OLIVEIRA MELLO	26/01/1943	LYRA COSTA DE OLIVEIRA
THEREZA LIMA DOS SANTOS	30/06/1938	MARIA FAGUNES
THEREZA MARIA MENDES DOS SANTOS	15/10/1945	MARIA INES DE JESUS MENDES
THEREZA MARIA PINTO DO AMARAL	20/11/1940	PRECIOSA PEREIRA RAMOS DE CARVALHO
THEREZA VIANNA DA SILVA	22/10/1935	JULIETA BRAZ DA SILVA
THEREZINHA ALBERTINA DE JESUS BERTOLOTI	14/11/1933	MARIA GELMIRA DE MENEZES
THEREZINHA BRANCO DE SOUZA	23/09/1933	MARIA DO ROSARIO BRANCO
THEREZINHA DE JESUS COELHO XAVIER	13/08/1933	JOSEPHINA MORELLI
THEREZINHA DE JESUS DO AMARAL PEREIRA	25/02/1930	CATHARINA KAPPAUM DO AMARAL
THEREZINHA DE JESUS MARQUES CORREA BLATT	25/04/1941	CARMELITA ASSUMPCAO MARQUES CORREA
THEREZINHA FERNANDES VIANNA	19/09/1940	ELIZA LUCILHA TEFCH VIANNA
THEREZINHA GONCALVES PESSURNO	24/08/1939	DULCE GASPAR GONCALVES
THEREZINHA MARIA MATHIAS FONSECA	06/02/1937	ANNA CECILIA NIEBUS MATHIAS
THEREZINHA MARIA MATHIAS FONSECA	06/02/1937	ANNA CECILIA NIEBUS MATHIAS
THEREZINHA PAES DE ALMEIDA	29/08/1933	CARLOTA SANTOS DE ALMEIDA
THEREZINHA PINHEIRO RODRIGUES	09/12/1930	CLOTILDE PINHEIRO RODRIGUES
THEREZINHA RODRIGUES DA COSTA	23/02/1932	ANTONIA CARVALHO DA COSTA
THEREZINHA VIEIRA	08/06/1936	MARIA FRANCISCA VIEIRA
TUGUO YAMAMOTO	22/06/1940	TUGUIKU YAMAMOTO
VALDAIR ROSA SOARES CASESKY	08/07/1946	NADIR ROSA SOARES
VALDEA MIRANDA DOS SANTOS	13/06/1943	PAULINA DA SILVA MIRANDA
VALDEMIRO URBANO	21/02/1948	THEREZA GALDINO DE OLIVEIRA
VALDETE DE OLIVEIRA BRAGA	13/09/1944	TEREZA HAN DE OLIVEIRA
VALDEVINO RIBEIRO DE SOUZA	20/09/1935	HELENA MARIA DE SOUZA
VALDIR ALVES NOGUEIRA	28/06/1947	FLORISA ALVES NOGUEIRA
VALDIR BIZZO VERGETTE	03/01/1939	EMILIA MARIA BIZZO VERGENTE
VALDIR DE OLIVEIRA FILHO	22/10/1948	DIB JOSE DE OLIVEIRA
VALDIR FRANCISCO MARCOLINO	16/06/1944	ALDA SILVA PORTO MARCOLINO

#3 *Directory Listing*

Ao selecionar o usuário "TESTE TESTE", conseguimos realizar o Agendamento para Foto desse usuário em questão (vide imagem 4). Entendemos que seria possível realizar esse tipo de procedimento para todos os demais usuários listados nessa página (listado na imagem 3).

Imagem 4


www.riocard.com/usuario/petropolis_cad_senior/agenda_ajax/agenda.asp
Home
Sair
RIOCard
Tudo anda melhor
Agendar Foto
Solicitar Entrega
RIOCard SÊNIOR
Maria de Souza
123.456.789-00
12-34-5678999-9
Finalizar
Portal Riocard

Agendamento para Foto

Sr(a) TESTE TESTE, a sua foto está agendada para o dia **06/01/2015** às **13:30**, no posto localizado na:

Praca da Inconfidencia, 16
CENTRO - Proximo a Igreja do Rosario

Não é necessário chegar antes do horário.

O próprio usuário deve estar presente com os seguintes documentos originais:

Identidade, CPF e Comprovante de Residência atual, de até 3 meses atrás - Conta de água, luz, gás ou telefone.

Se o comprovante estiver no nome de outra pessoa, será necessário apresentar também:
- Certidão de Casamento original, ou registro de união estável: se residir com Esposa/Marido;
- Certidão de Nascimento ou Identidade do(a) filho(a) original: se residir com filhos;
- Certidão de Nascimento do(a) neto(a): se residir com netos;
- O próprio documento de identificação: se residir com os pais.

Se o comprovante estiver no nome de terceiro, sem parentesco, deverá ser apresentada uma declaração com reconhecimento de firma em cartório, declarando que o usuário reside no endereço informado. A declaração deve ser original e tem validade de 30 dias a contar da data de sua emissão.

Caso não possa comparecer na data agendada, será necessário reagendar.

Dados da sua conexão:
IP: 198.143.41.65
Host: 198.143.41.65

Recomendação	É recomendada a avaliação da necessidade de listagem de arquivos, com o objetivo de garantir que esses arquivos não exponham informações que possam ser utilizadas por um usuário mal intencionado. Recomendamos que não seja possível habilitar a listagem de diretórios nas configurações do *Web Server*.
Data do Teste	04/11/2014
Tipo de Teste Executado	Manipulação de URLs

#4 *CAPTCHA Validation in the Client Side*

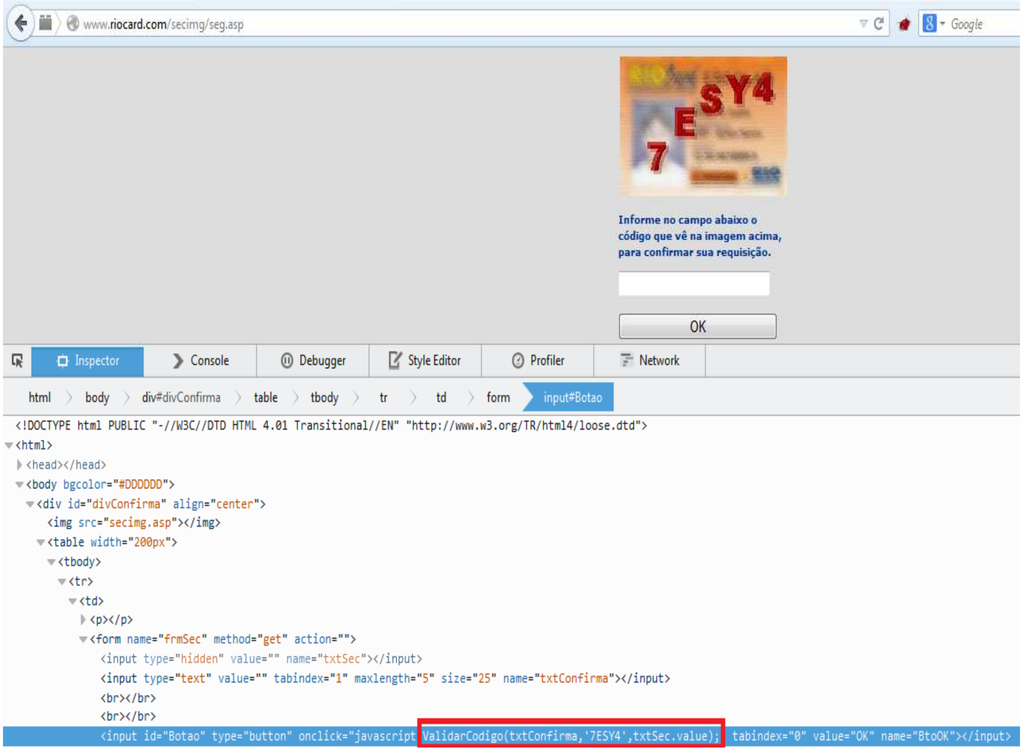
Descrição da Vulnerabilidade

Código do Captcha está facilmente acessível no código HTML da página, podendo ser explorado por ferramentas automatizadas.

CAPTCHA ("**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part") é um tipo de teste usado para determinar se o usuário é ou não humano, ou seja, limitando que a entrada de dados seja realizada pelo teclado ou da tela do computador.

URLs Afetados	http://www.riocard.com/secimg/seg.asp
Impacto	Por meio de ferramentas automatizadas seria possível realizar uma auto resolução do CAPTCHA, tornando possível realizar técnicas de *brute-force*
Severidade	Médio

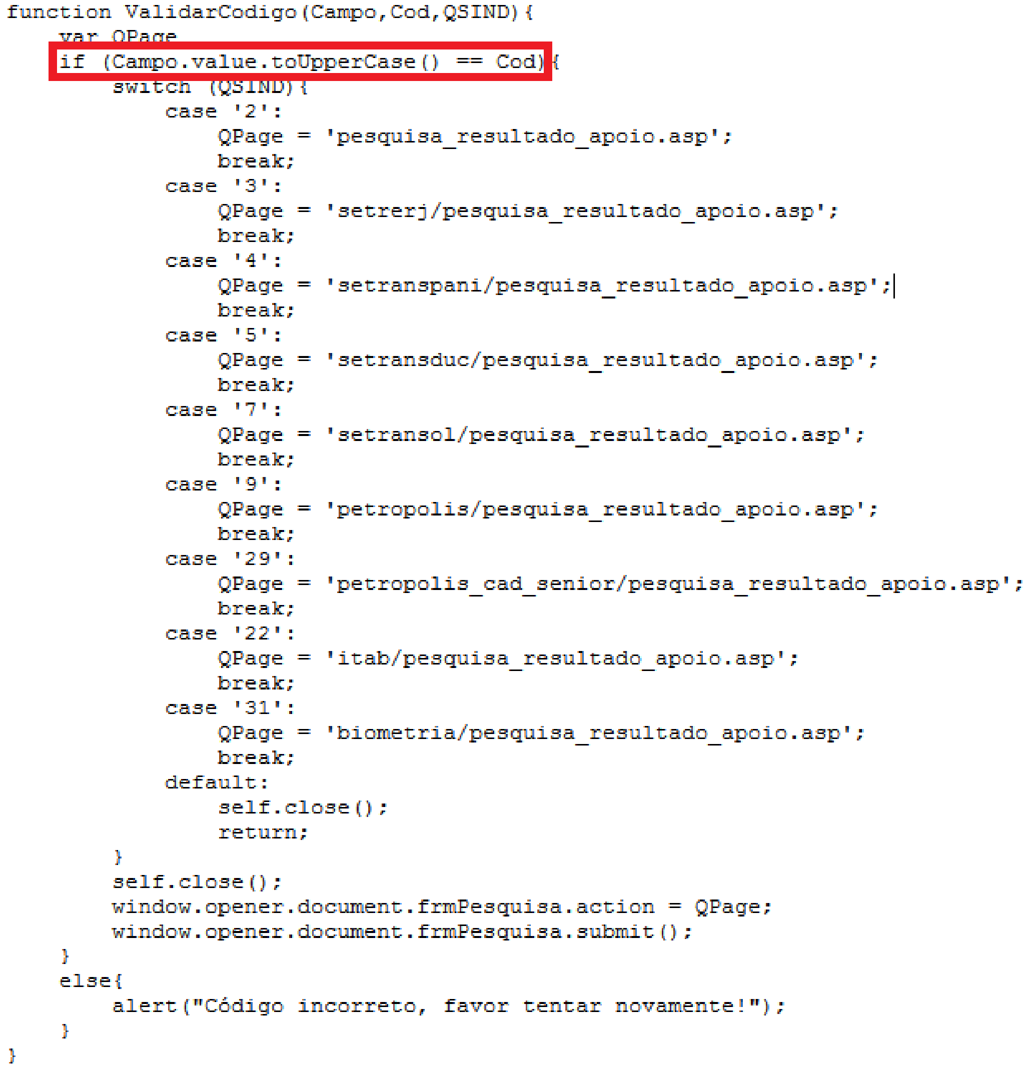
Evidência


www.riocard.com/secimg/seg.asp
Google
7ESY4
OK
Inspector
Console
Debugger
Style Editor
Profiler
Network
html
body
div#divConfirma
table
tbody
tr
td
form
input#Botao

Informe no campo abaixo o código que vê na imagem acima, para confirmar sua requisição.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
  <head></head>
  <body bgcolor="#DDDDDD">
    <div id="divConfirma" align="center">
      <img src="secimg.asp"></img>
      <table width="200px">
        <tbody>
          <tr>
            <td>
              <p></p>
              <form name="frmSec" method="get" action="">
                <input type="hidden" value="" name="txtSec"></input>
                <input type="text" value="" tabindex="1" maxlength="5" size="25" name="txtConfirma"></input>
                <br></br>
                <br></br>
                <input id="Botao" type="button" onclick="javascript ValidarCodigo(txtConfirma,'7ESY4',txtSec.value);  tabindex="0" value="OK" name="BtoOK"></input>
```

#3	*Directory Listing*



```
function ValidarCodigo(Campo,Cod,QSIND){
    var QPage
    if (Campo.value.toUpperCase() == Cod){
        switch (QSIND){
            case '2':
                QPage = 'pesquisa_resultado_apoio.asp';
                break;
            case '3':
                QPage = 'setrerj/pesquisa_resultado_apoio.asp';
                break;
            case '4':
                QPage = 'setranspani/pesquisa_resultado_apoio.asp';
                break;
            case '5':
                QPage = 'setransduc/pesquisa_resultado_apoio.asp';
                break;
            case '7':
                QPage = 'setransol/pesquisa_resultado_apoio.asp';
                break;
            case '9':
                QPage = 'petropolis/pesquisa_resultado_apoio.asp';
                break;
            case '29':
                QPage = 'petropolis_cad_senior/pesquisa_resultado_apoio.asp';
                break;
            case '22':
                QPage = 'itab/pesquisa_resultado_apoio.asp';
                break;
            case '31':
                QPage = 'biometria/pesquisa_resultado_apoio.asp';
                break;
            default:
                self.close();
                return;
        }
        self.close();
        window.opener.document.frmPesquisa.action = QPage;
        window.opener.document.frmPesquisa.submit();
    }
    else{
        alert("Código incorreto, favor tentar novamente!");
    }
}
```

Recomendação	É recomendado que a verificação do CAPTCHA deva ser feito no servidor sem ser exposto ao lado cliente da comunicação (nas estações de trabalho).
Data do Teste	06/11/2014
Tipo de Teste Executado	Análise do código-fonte HTML da página web

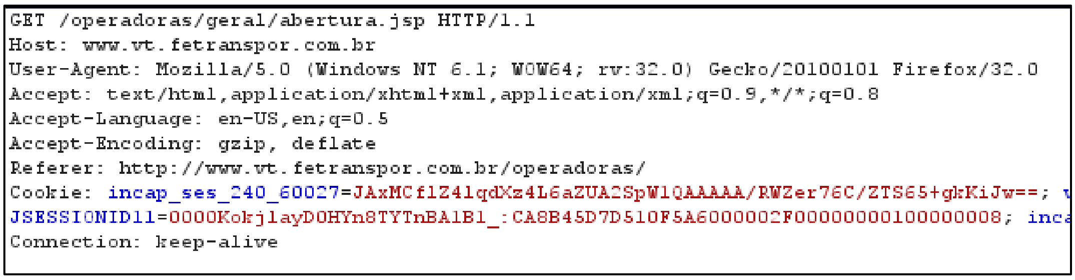
#5 *Clickjacking: X-Frame-Options header missing*

Descrição da Vulnerabilidade

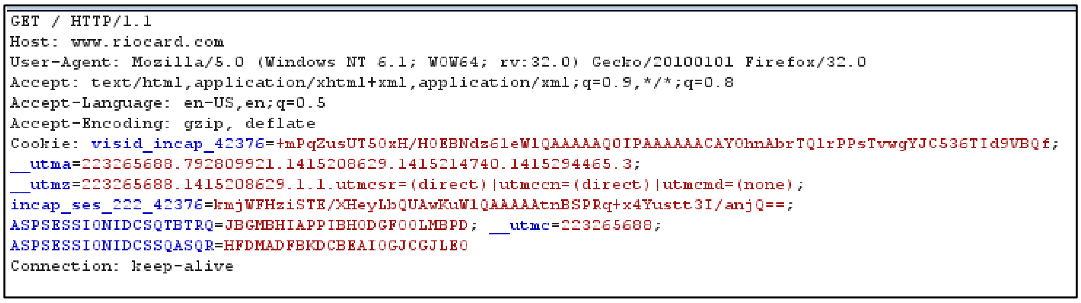
Clickjacking é uma técnica utilizada por atacantes para enganar usuários comuns a clicarem em links ou objetos maliciosos, ou até mesmo, alterar os links genuínos por esses objetos. Essa técnica pode levar ao vazamento de informações confidenciais ou até mesmo levar ao controle do computador do usuário enquanto o mesmo clica em páginas *web* aparentemente inocentes.

URLs Afetados	http://www.vt.fetranspor.com.br/operadoras/ http://www.riocard.com https://www.cartaoriocard.com.br
Impacto	O servidor não retornou um cabeçalho X-frame-Options. Isto significa que este site pode estar em risco de um ataque de clickjacking. O cabeçalho de resposta HTTP X-Frame-Options pode ser usado para indicar ou não se um navegador deve ser autorizado a renderizar uma página em um <frame> ou <iframe>. Os sites podem usar isso para evitar ataques clickjacking, assegurando que o seu conteúdo não é incorporado outros sites.
Severidade	Baixo

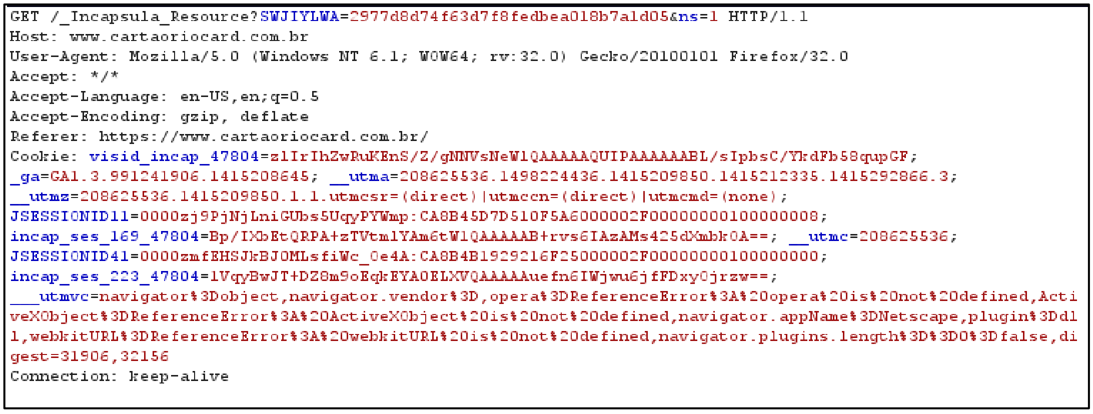
Evidência



```
GET /operadoras/geral/abertura.jsp HTTP/1.1
Host: www.vt.fetranspor.com.br
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.vt.fetranspor.com.br/operadoras/
Cookie: incap_ses_240_60027=JAxMCf1Z41qdXz4L6aZUA2SpW1QAAAAA/RWZer76C/ZTS65+gkKiJw==; 
JSESSIONID11=0000KokjlayDOHYn8TYTnBA1B1_:CA8B45D7D510F5A6000002F00000000100000008; inca
Connection: keep-alive
```



```
GET / HTTP/1.1
Host: www.riocard.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: visid_incap_42376=+mPqZusUT50xH/H0EBNdz6leW1QAAAAAQ0IPAAAAAACAY0hnAbrTQlrPPsTvwgYJC536TId9VBQf;
__utma=223265688.792809921.1415208629.1415214740.1415294465.3;
__utmz=223265688.1415208629.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
incap_ses_222_42376=kmjWFHziSTE/XHeyLbQUAwKuW1QAAAAAtnBSPRq+x4Yustt3I/anjQ==;
ASPSESSIONIDCSQTBTRQ=JBGMBHIAPPIBHODGFOOLMBPD; __utmc=223265688;
ASPSESSIONIDCSSQASQR=HFDMADFBKDCBEAIOGJCGJLEO
Connection: keep-alive
```

#5	***Clickjacking: X-Frame-Options header missing***
	

```
GET /_Incapsula_Resource?SWJIYLWA=2977d8d74f63d7f8fedbea018b7a1d05&ns=1 HTTP/1.1
Host: www.cartaoriocard.com.br
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.cartaoriocard.com.br/
Cookie: visid_incap_47804=zlIrIhZwRuKEnS/Z/gMNVsNeW1QAAAAAQUIPAAAAAABL/sIpbsC/YkdFb58qupGF;
_ga=GA1.3.991241906.1415208645; __utma=208625536.1498224436.1415209850.1415212335.1415292866.3;
__utmz=208625536.1415209850.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
JSESSIONID11=0000zj9PjNjLniGUbs5UqyPYWmp:CA8B45D7D510F5A6000002F00000000100000008;
incap_ses_169_47804=Bp/IXbEtQRPA+zTVtmlYAm6tW1QAAAAAB+rvs6IAzAMs425dXmbk0A==; __utmc=208625536;
JSESSIONID41=0000zmfEHSJkBJOMLsfiWc_0e4A:CA8B4B1929216F25000002F00000000100000000;
incap_ses_223_47804=1VqyBwJT+DZ8m9oEqkEYA0ELXVQAAAAAuefn6IWjwu6jfFDxy0jrzw==;
___utmvc=navigator%3Dobject,navigator.vendor%3D,opera%3DReferenceError%3A%20opera%20is%20not%20defined,Acti
veXObject%3DReferenceError%3A%20ActiveXObject%20is%20not%20defined,navigator.appName%3DNetscape,plugin%3Ddl
l,webkitURL%3DReferenceError%3A%20webkitURL%20is%20not%20defined,navigator.plugins.length%3D%3D0%3Dfalse,di
gest=31906,32156
Connection: keep-alive
```

Recomendação	É recomendado configurar seu servidor web para incluir um cabeçalho X-frame-Options
Data do Teste	07/11/2014
Tipo de Teste Executado	Análise de *flags* do pacote HTTP

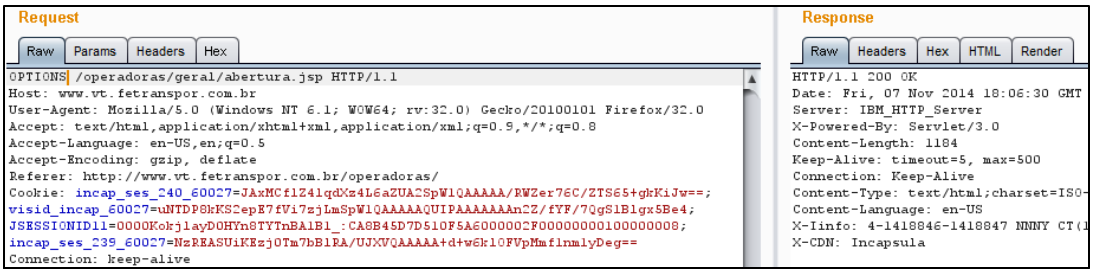
#6 *OPTIONS method is enabled*

Descrição da Vulnerabilidade

O método HTTP OPTIONS está habilitado para este web server. Este método fornece uma lista de métodos que são suportados pelo *web server* apresentando uma lista de opções de comunicação disponíveis nas requisições e respostas aceitas pela Request-URI.

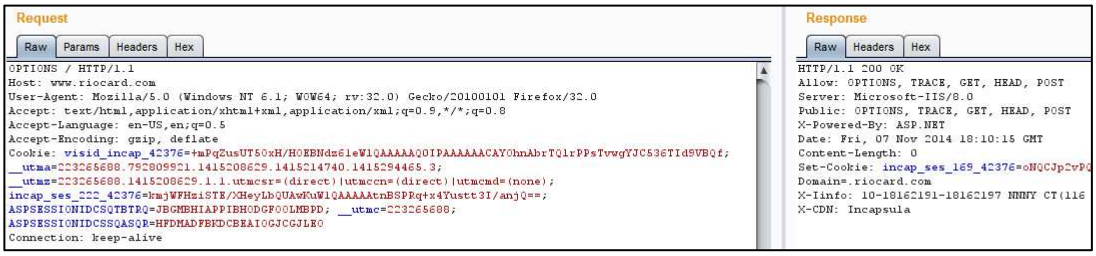
URLs Afetados	http://www.vt.fetranspor.com.br/operadoras/ http://www.riocard.com https://www.cartaoriocard.com.br
Impacto	Informações sensíveis sobre o funcionamento do *web server* podem ser expostas a usuários maliciosos, apresentando vetores de ataques mais avançados
Severidade	Baixo

Evidência



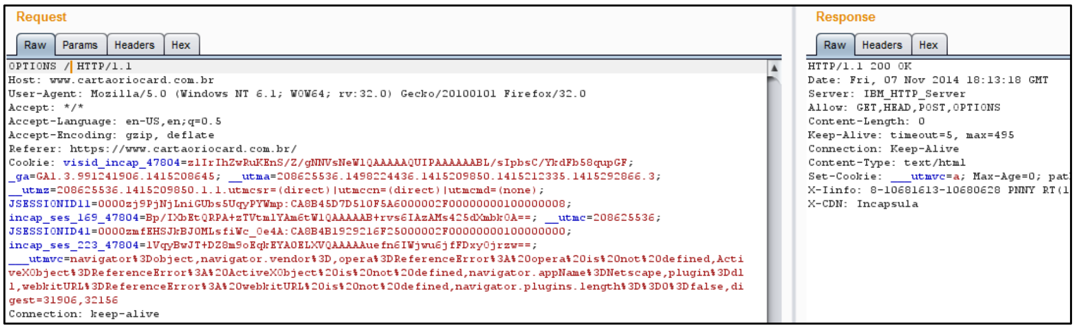
```
OPTIONS /operadoras/geral/abertura.jsp HTTP/1.1
Host: www.vt.fetranspor.com.br
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.vt.fetranspor.com.br/operadoras/
Cookie: incap_ses_240_60027=JAxMCf1Z41qdXz4L6aZUA2SpW1QAAAAA/RWZer76C/ZTS65+gkKiJw==;
visid_incap_60027=uNTDP8kKS2epE7fVi7zjLmSpW1QAAAAAQUIPAAAAAAAn2Z/fYF/7QgS1B1gx5Be4;
JSESSIONID11=0000KokjlayD0HYn8TYTnBA1B1_:CA8B45D7D510F5A6000002F00000000100000008;
incap_ses_239_60027=NzREASUiKEzj0Tm7bB1RA/UJXVQAAAAA+d+w6kl0FVpMmflnmlyDeg==
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Fri, 07 Nov 2014 18:06:30 GMT
Server: IBM_HTTP_Server
X-Powered-By: Servlet/3.0
Content-Length: 1184
Keep-Alive: timeout=5, max=500
Connection: Keep-Alive
Content-Type: text/html;charset=ISO-
Content-Language: en-US
X-Iinfo: 4-1418846-1418847 NNNY CT(1
X-CDN: Incapsula
```



```
OPTIONS / HTTP/1.1
Host: www.riocard.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: visid_incap_42376=+mPqZusUT50xH/H0EBNdz6leW1QAAAAAQ0IPAAAAAACAY0hnAbrTQ1rPPsTvwgYJC536TId9VBQf;
__utma=223265688.792809921.1415208629.1415214740.1415294465.3;
__utmz=223265688.1415208629.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
incap_ses_222_42376=kmjWFHziSTE/XHeyLbQUAwKuW1QAAAAAtnBSPRq+x4Yustt3I/anjQ==;
ASPSESSIONIDCSQTBTRQ=JBGMBHIAPPIBH0DGF00LMBPD; __utmc=223265688;
ASPSESSIONIDCSSQASQR=HFDMADFBKDCBEAI0GJCGJLE0
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Allow: OPTIONS, TRACE, GET, HEAD, POST
Server: Microsoft-IIS/8.0
Public: OPTIONS, TRACE, GET, HEAD, POST
X-Powered-By: ASP.NET
Date: Fri, 07 Nov 2014 18:10:15 GMT
Content-Length: 0
Set-Cookie: incap_ses_169_42376=oNQCJp2vPQ
Domain=.riocard.com
X-Iinfo: 10-18162191-18162197 NNNY CT(116
X-CDN: Incapsula
```

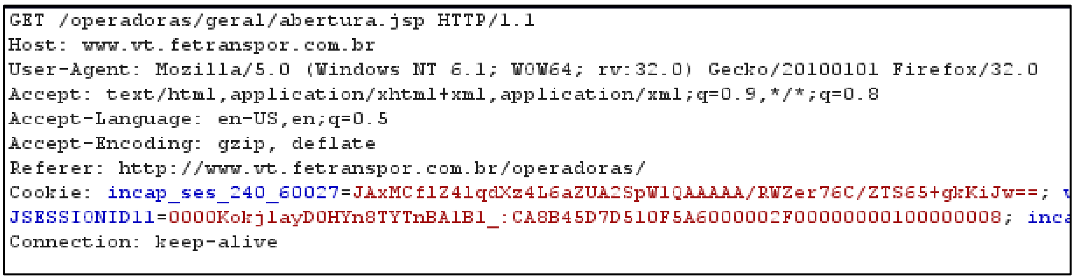


```
OPTIONS / HTTP/1.1
Host: www.cartaoriocard.com.br
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.cartaoriocard.com.br/
Cookie: visid_incap_47804=zlIrIhZwRuKEnS/Z/gNNVsNeW1QAAAAAQUIPAAAAAABL/sIpbsC/YkdFb58qupGF;
_ga=GA1.3.991241906.1415208645; __utma=208625536.1498224436.1415209850.1415212335.1415292866.3;
__utmz=208625536.1415209850.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
JSESSIONID11=0000zj9PjNjLniGUbs5UqyPYWmp:CA8B45D7D510F5A6000002F00000000100000008;
incap_ses_169_47804=Bp/IXbEtQRPA+zTVtmlYAm6tW1QAAAAAB+rvs6IAzAMs425dXmbk0A==; __utmc=208625536;
JSESSIONID41=0000zmfEHSJkBJ0MLsfiWc_0e4A:CA8B4B1929216F25000002F00000000100000000;
incap_ses_223_47804=1VqyBwJT+DZ8m9oEqkEYA0ELXVQAAAAAuefn6IWjwu6jfFDxy0jrzw==;
___utmvc=navigator%3Dobject,navigator.vendor%3D,opera%3DReferenceError%3A%20opera%20is%20not%20defined,Acti
veXObject%3DReferenceError%3A%20ActiveXObject%20is%20not%20defined,navigator.appName%3DNetscape,plugin%3Ddl
l,webkitURL%3DReferenceError%3A%20webkitURL%20is%20not%20defined,navigator.plugins.length%3D%3D0%3Dfalse,di
gest=31906,32156
Connection: keep-alive
```

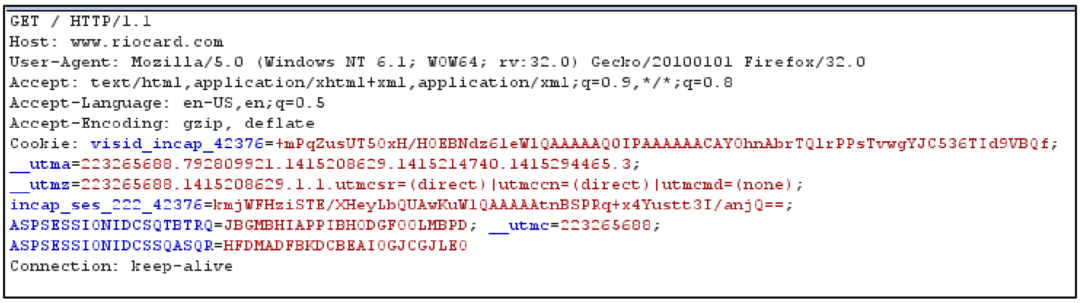
```
HTTP/1.1 200 OK
Date: Fri, 07 Nov 2014 18:13:18 GMT
Server: IBM_HTTP_Server
Allow: GET,HEAD,POST,OPTIONS
Content-Length: 0
Keep-Alive: timeout=5, max=495
Connection: Keep-Alive
Content-Type: text/html
Set-Cookie: ___utmvc=a; Max-Age=0; pat
X-Iinfo: 8-10681613-10680628 PNNY RT(1
X-CDN: Incapsula
```

Recomendação	É recomendável se desabilitar todos os métodos não necessários e de desenvolvimento para sites de produção.

#6	*OPTIONS method is enabled*
Data do Teste	07/11/2014
Tipo de Teste Executado	Análise da resposta do método OPTIONS

#7	Session Cookie without HttpOnly flag set
Descrição da Vulnerabilidade A sinalização HTTPOnly instrui o navegador de que os cookies só podem ser acessados pelo servidor, se tornando inacessíveis pelo navegador do client. Essa sinalização é uma medida de segurança para proteção de cookies de sessão e autenticação.	
URLs Afetados	http://www.vt.fetranspor.com.br/operadoras/ http://www.riocard.com
Impacto	Usuários mal intencionados podem utilizar esses cookies para executar ataques, roubar contas de usuários ou realizar scans automatizado em zonas autenticadas
Severidade	Baixo
Evidência	

```
GET /operadoras/geral/abertura.jsp HTTP/1.1
Host: www.vt.fetranspor.com.br
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.vt.fetranspor.com.br/operadoras/
Cookie: incap_ses_240_60027=JAxMCflZ4lqdXz4L6aZUA2SpW1QAAAAA/RWZer76C/ZTS65+gkKiJw==;
JSESSIONID11=0000KokjlayD0HYn8TYTnBA1B1_:CA8B45D7D510F5A6000002F00000000100000008; inca
Connection: keep-alive
```

#6	***OPTIONS method is enabled***
	

```
GET / HTTP/1.1
Host: www.riocard.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: visid_incap_42376=+mPqZusUT50xH/H0EBNdz6leW1QAAAAAQ0IPAAAAAACAY0hnAbrTQlrPPsTvwgYJC536TId9VBQf;
__utma=223265688.792809921.1415208629.1415214740.1415294465.3;
__utmz=223265688.1415208629.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
incap_ses_222_42376=kmjWFHziSTE/XHeyLbQUAwKuW1QAAAAAtnBSPRq+x4Yustt3I/anjQ==;
ASPSESSIONIDCSQTBTRQ=JBGMBHIAPPIBHODGFOOLMBPD; __utmc=223265688;
ASPSESSIONIDCSSQASQR=HFDMADFBKDCBEAIOGJCGJLEO
Connection: keep-alive
```

Recomendação	Sugerimos a habilitação do HTTPOnly para aprimorar a proteção dos cookies de sessão de sua aplicação.
Data do Teste	07/11/2014
Tipo de Teste Executado	Manipulação de Cookies

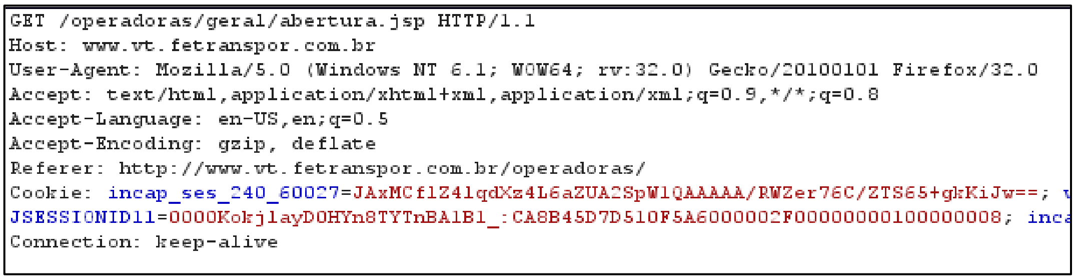
#8 *Session Cookie without Secure flag set*

Descrição da Vulnerabilidade

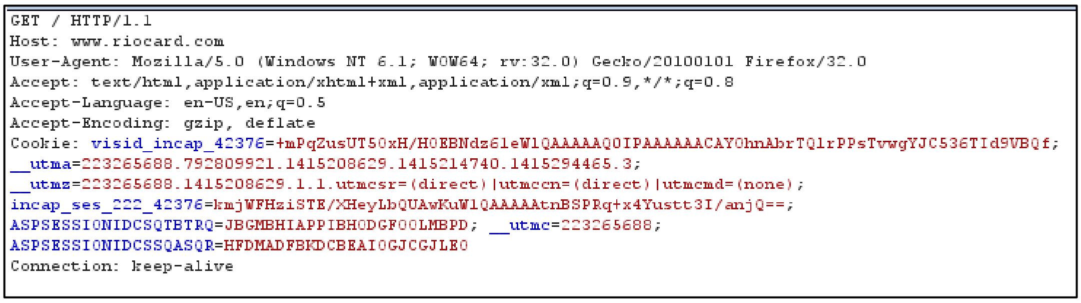
A sinalização de segurança (Secure flag) do Cookie não está configurada. Essa sinalização no Cookie indica ao navegador que o Cookie só pode ser acessado por meio de canais seguros SSL. Essa configuração é importante para se proteger os Cookies de Sessão de uma aplicação.

URLs Afetados	http://www.vt.fetranspor.com.br/operadoras/ http://www.riocard.com
Impacto	Os *cookies* podem ser visualizados por terceiros não autorizados, devido à transmissão de dos dados em texto claro.
Severidade	Baixo

Evidência



```
GET /operadoras/geral/abertura.jsp HTTP/1.1
Host: www.vt.fetranspor.com.br
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.vt.fetranspor.com.br/operadoras/
Cookie: incap_ses_240_60027=JAxMCf1Z41qdXz4L6aZUA2SpW1QAAAAA/RWZer76C/ZTS65+gkKiJw==;
JSESSIONID11=0000KokjlayDOHYn8TYTnBA1B1_:CA8B45D7D510F5A6000002F00000000100000008; inca
Connection: keep-alive
```



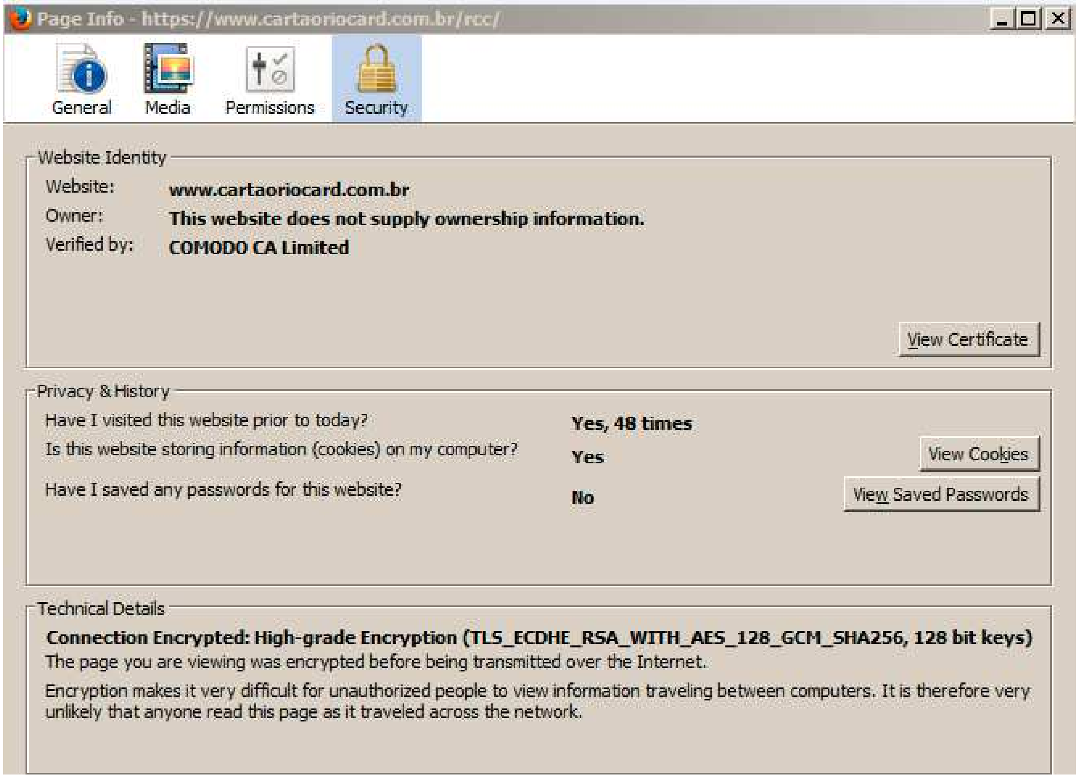
```
GET / HTTP/1.1
Host: www.riocard.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: visid_incap_42376=+mPqZusUT50xH/H0EBNdz61eW1QAAAAAQ0IPAAAAAACAY0hnAbrTQ1rPPsTvwgYJC536TId9VBQf;
__utma=223265688.792809921.1415208629.1415214740.1415294465.3;
__utmz=223265688.1415208629.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
incap_ses_222_42376=kmjWFHziSTE/XHeyLbQUAwKuW1QAAAAAtnBSPRq+x4Yustt3I/anjQ==;
ASPSESSIONIDCSQTBTRQ=JBGMBHIAPPIBHODGFOOLMBPD; __utmc=223265688;
ASPSESSIONIDCSSQASQR=HFDMADFBKDCBEAIOGJCGJLEO
Connection: keep-alive
```

Recomendação	É recomendado colocar a Secure flag para esse cookie.
Data do Teste	07/11/2014
Tipo de Teste Executado	Manipulação de Cookies

#9 *TLS1/SSLv3 Renegotiation Vulnerability*

Descrição da Vulnerabilidade

Uma vulnerabilidade nos protocolos SSL e TLS permite pedidos de renegociação que pode permitir a invasor injetar texto simples em um *stream* de protocolo de aplicação. Esse problema afeta SSL versão 3.0 e mais recentes e TLS versão 1.0 e mais recentes.

URLs Afetados	https://www.cartaoriocard.com.br
Impacto	Possibilidade de envio de comandos por um atacante para o ambiente tecnológico que parecem estar vindo de uma fonte legítima.
Severidade	Médio
Evidência	

Website Identity

Website: www.cartaoriocard.com.br
Owner: This website does not supply ownership information.
Verified by: COMODO CA Limited

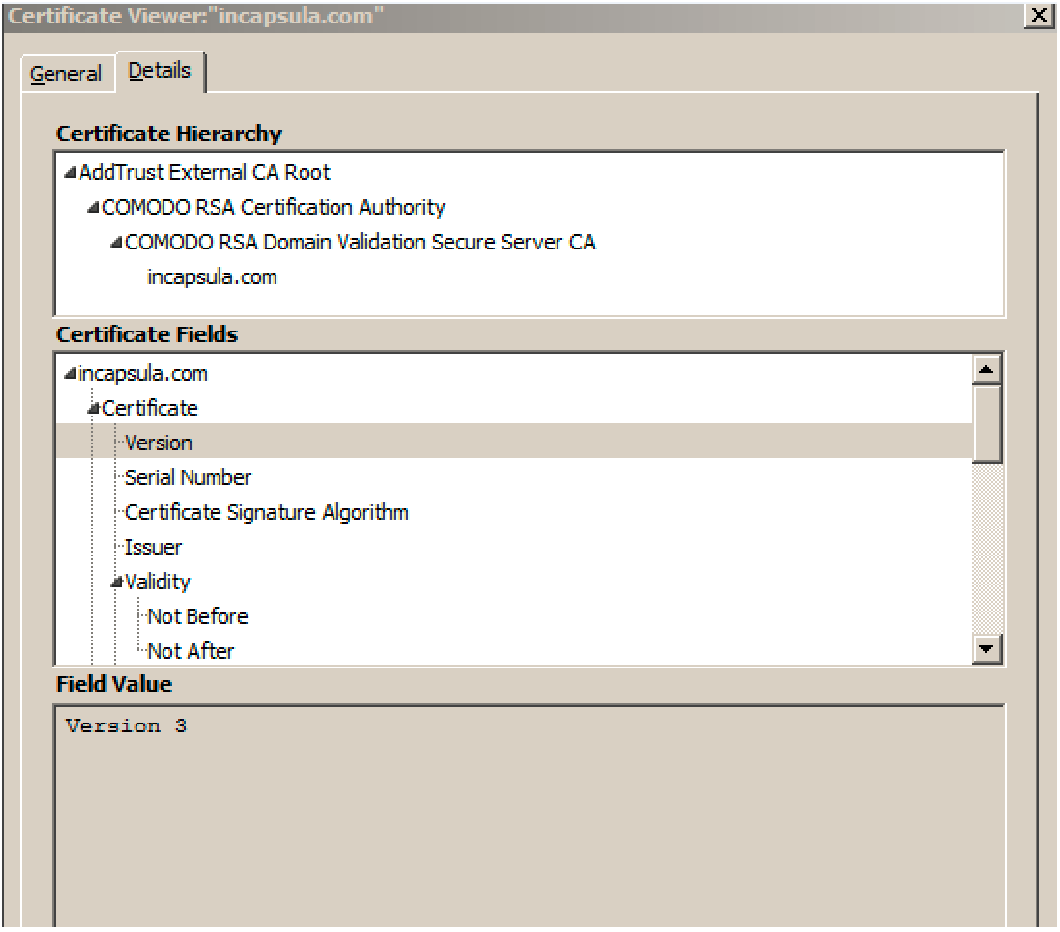
Privacy & History

Have I visited this website prior to today? Yes, 48 times
Is this website storing information (cookies) on my computer? Yes
Have I saved any passwords for this website? No

Technical Details

Connection Encrypted: High-grade Encryption (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

#9 *TLS1/SSLv3 Renegotiation Vulnerability*



Certificate Hierarchy

- AddTrust External CA Root
  - COMODO RSA Certification Authority
    - COMODO RSA Domain Validation Secure Server CA
      - incapsula.com

Certificate Fields

- incapsula.com
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before
      - Not After

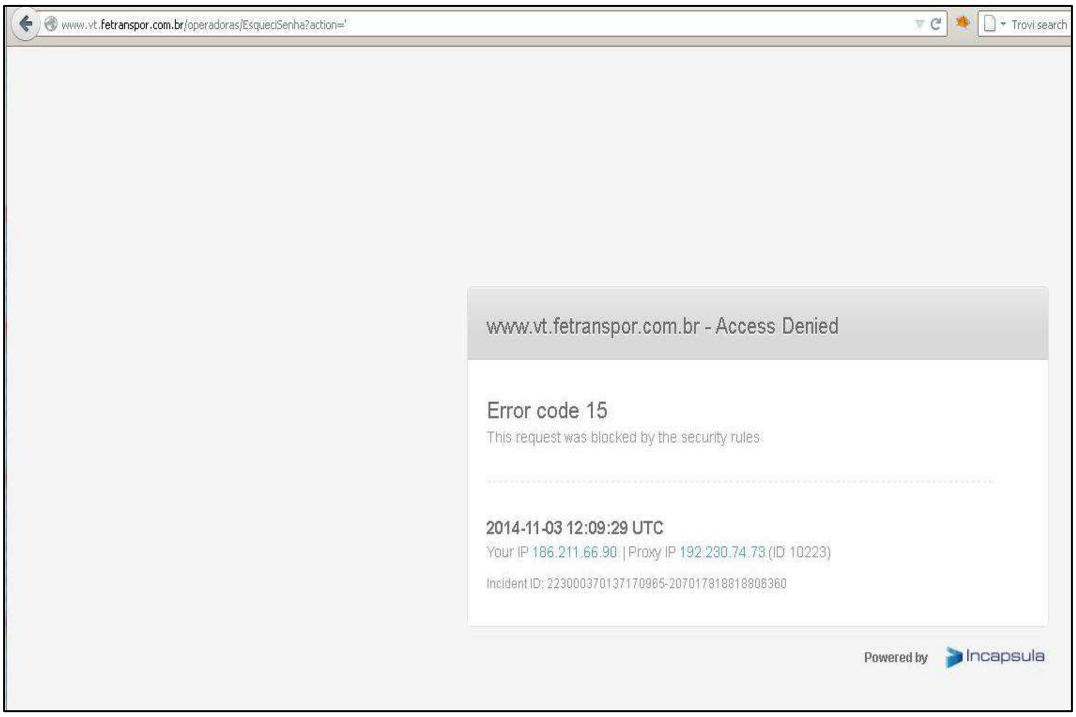
Field Value

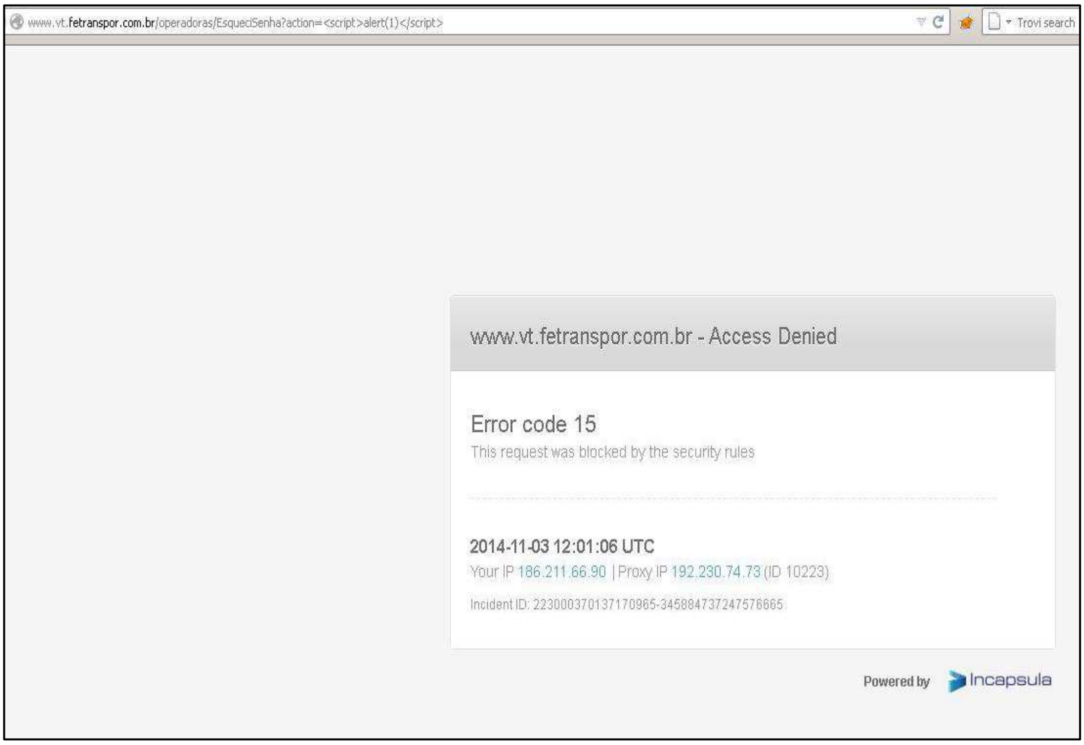
```
Version 3
```

Recomendação	A causa da vulnerabilidade pode depender de aplicação para aplicação, uma análise mais profunda deve ser realizada para a correção do problema. É recomendável entrar em contato com o responsável pela aplicação para a correção do problema.
Data do Teste	07/11/2014
Tipo de Teste Executado	*Code Injection*

(c) Validações Manuais de Vulnerabilidades Sem Sucesso

Abaixo listamos os principais testes que foram realizados de forma manual, porém sem sucesso.

1.	**SQL Injection**
Resultado Obtido	Não obtivemos sucesso na exploração dessa vulnerabilidade, pois o Firewall de Aplicação (Incapsula) bloqueou as requisições maliciosas, chegando até a bloquear o endereço IP de onde partiam tais requisições.
Tipo de teste executado	SQL Injection
Evidência	 www.vt.fetranspor.com.br/operadoras/EsqueciSenha?action=' www.vt.fetranspor.com.br - Access Denied Error code 15 This request was blocked by the security rules 2014-11-03 12:09:29 UTC Your IP 186.211.66.90 | Proxy IP 192.230.74.73 (ID 10223) Incident ID: 223000370137170965-207017818818806360 Powered by Incapsula
2.	**Cross Site Scripting**
Resultado Obtido	Não obtivemos sucesso na exploração dessa vulnerabilidade, pois o Firewall de Aplicação (Incapsula) bloqueou as requisições maliciosas, chegando até a bloquear o endereço IP de onde partiam tais requisições.
Tipo de teste executado	XSS (Cross-Site Scripting)
Evidência	

www.vt.fetranspor.com.br/operadoras/EsqueciSenha?action=<script>alert(1)</script>

www.vt.fetranspor.com.br - Access Denied

Error code 15

This request was blocked by the security rules

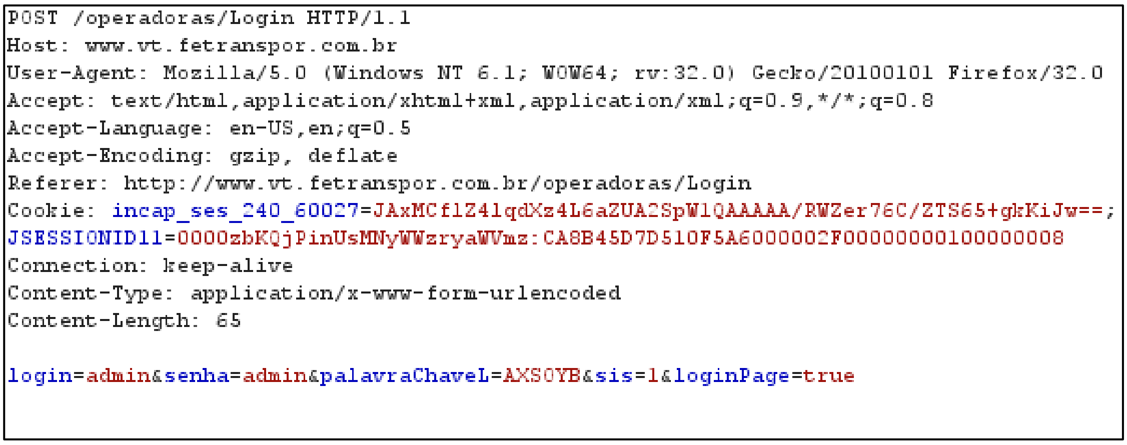
2014-11-03 12:01:06 UTC

Your IP 186.211.66.90 | Proxy IP 192.230.74.73 (ID 10223)

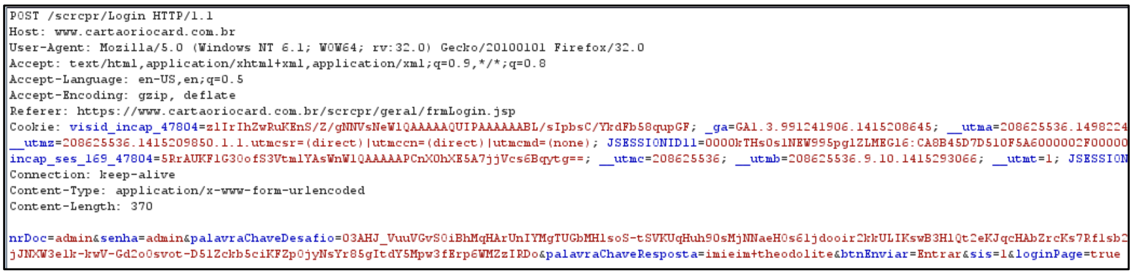
Incident ID: 223000370137170965-345884737247576665

3.	Autenticação com credenciais padrão
Resultado Obtido	Tentamos nos autenticar nos sites em escopo com a utilização de credenciais padrão, que normalmente são utilizadas como, por exemplo, usuário e senha “admin”. No entanto, não obtivemos sucesso.
Tipo de teste	Uso de sessão de terceiros

Evidenciais



```
POST /operadoras/Login HTTP/1.1
Host: www.vt.fetranspor.com.br
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.vt.fetranspor.com.br/operadoras/Login
Cookie: incap_ses_240_60027=JAxMCf1Z41qdXz4L6aZUA2SpW1QAAAAA/RWZer76C/ZTS65+gkKiJw==;
JSESSIONID11=0000zbKQjPinUsMNyWWzryaWVmz:CA8B45D7D510F5A6000002F00000000100000008
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

login=admin&senha=admin&palavraChaveL=AXS0YB&sis=1&loginPage=true
```

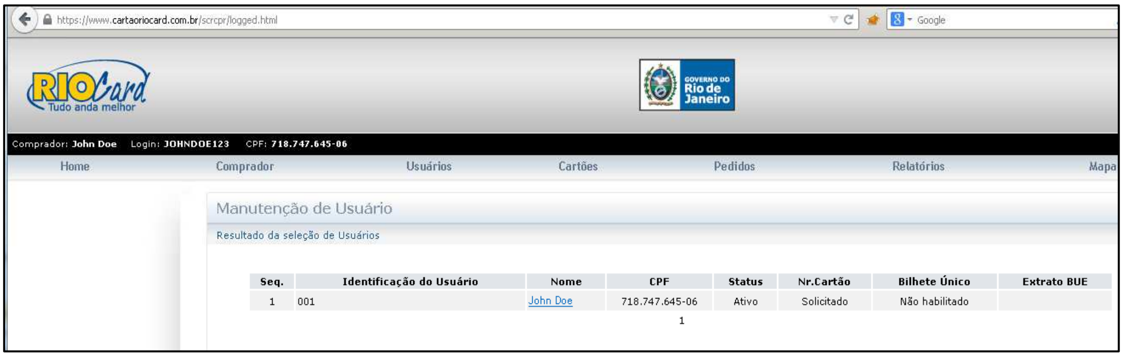


```
POST /scrcpr/Login HTTP/1.1
Host: www.cartaoriocard.com.br
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.cartaoriocard.com.br/scrcpr/geral/frmLogin.jsp
Cookie: visid_incap_47804=zlIrIhZwRuKEnS/Z/gNNVsNeW1QAAAAAQUIPAAAAAABL/sIpbsC/YkdFb58qupGF; _ga=GA1.3.991241906.1415208645; __utma=208625536.1498224
__utmz=208625536.1415209850.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); JSESSIONID11=0000kTHs0s1NEW995pglZLMEG16:CA8B45D7D510F5A6000002F00000
incap_ses_169_47804=5RrAUKF1G30ofS3VtmlYAsWnW1QAAAAAPCnX0hXE5A7jjVcs6Bqytg==; __utmc=208625536; __utmb=208625536.9.10.1415293066; __utmt=1; JSESSION
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 370

nrDoc=admin&senha=admin&palavraChaveDesafio=03AHJ_VuuVGvS0iBhMqHArUnIYMgTUGbMHlsoS-tSVKUqHuh90sMjNNaeH0s6ljdooir2kkULIKswB3HlQt2eKJqcHAbZrcKs7Rflsb2
jJNXW3elk-kwV-Gd2o0svot-D5lZckb5ciKFZp0jyNsYr85gItdY5Mpw3fErp6WMZzIRDo&palavraChaveResposta=imieim+theodolite&btnEnviar=Entrar&sis=1&loginPage=true
```

4. Manipulação de parâmetros de URL

Resultado Obtido	Tentamos alterar o código de usuário após estar autenticado no site https://cartaoriocard.com.br, a fim de acessar páginas não autorizadas, porém não obtivemos sucesso.
Tipo de teste executado	Manipulação de URLs

Evidências


https://www.cartaoriocard.com.br/scrcpr/logged.html
RIOCard
Tudo anda melhor
GOVERNO DO Rio de Janeiro
Home
Comprador
Usuários
Cartões
Pedidos
Relatórios
Mapa

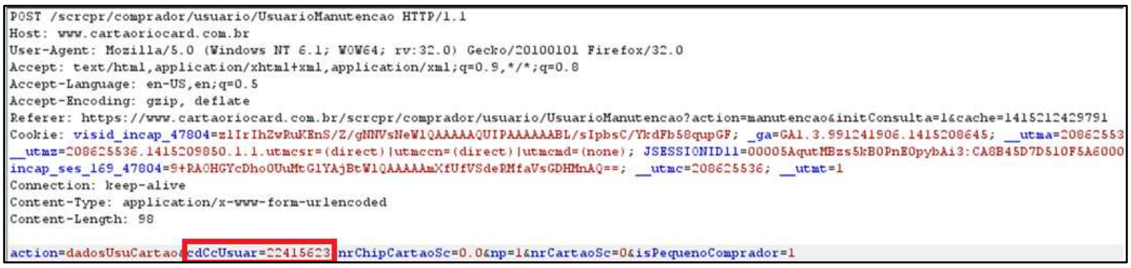
Comprador: John Doe Login: JOHNDOE123 CPF: 718.747.645-06

Manutenção de Usuário

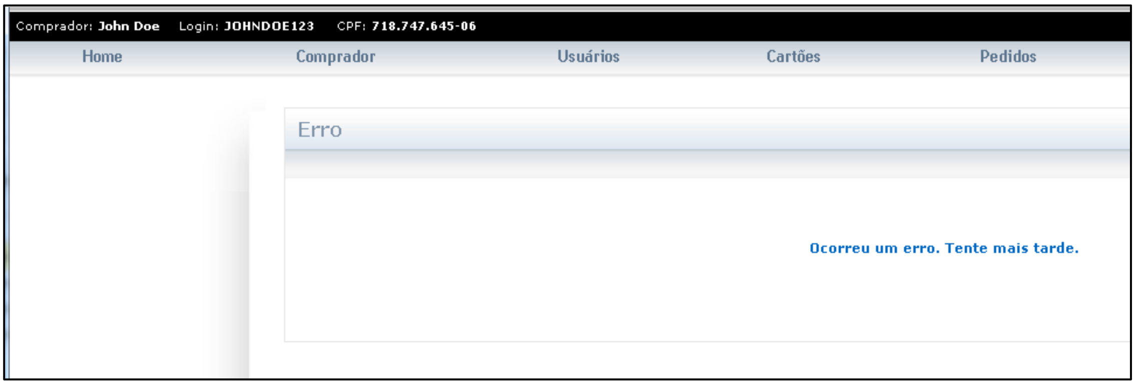
Resultado da seleção de Usuários

Seq.	Identificação do Usuário	Nome	CPF	Status	Nr.Cartão	Bilhete Único	Extrato BUE
1	001	John Doe	718.747.645-06	Ativo	Solicitado	Não habilitado	

1



```
POST /scrcpr/comprador/usuario/UsuarioManutencao HTTP/1.1
Host: www.cartaoriocard.com.br
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.cartaoriocard.com.br/scrcpr/comprador/usuario/UsuarioManutencao?action=manutencao&initConsulta=1&cache=1415212429791
Cookie: visid_incap_47804=zlIrIhZwRuKEnS/Z/gNNVsNeW1QAAAAAQUIPAAAAAABL/sIpbsC/YkdFb58qupGF; _ga=GA1.3.991241906.1415208645; __utma=20862553
__utmz=208625536.1415209850.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); JSESSIONID11=00005AqutMBzs5kB0PnE0pybAi3:CA8B45D7D510F5A6000
incap_ses_169_47804=9+RA0HGYcDhoOUuMtG1YAjBtW1QAAAAAmXfUfVSdeRMfaVsGDHMnAQ==; __utmc=208625536; __utmt=1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 98

action=dadosUsuCartao&cdCcUsuar=22415623&nrChipCartaoSc=0.0&np=1&nrCartaoSc=0&isPequenoComprador=1
```


Home
Comprador
Usuários
Cartões
Pedidos

Comprador: John Doe Login: JOHNDOE123 CPF: 718.747.645-06

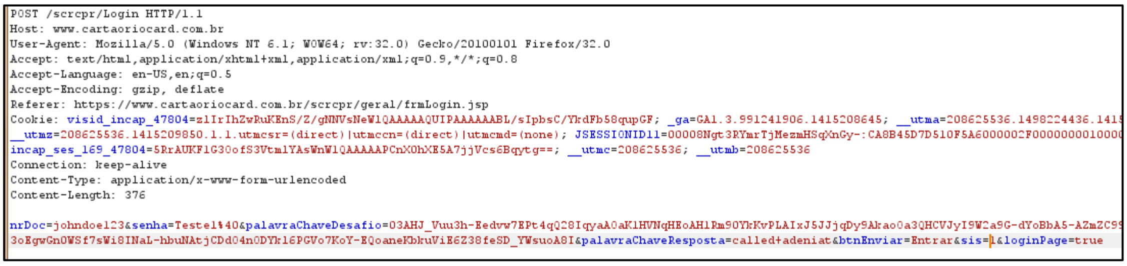
Erro

Ocorreu um erro. Tente mais tarde.

5. Escalação de privilégios

Resultados Obtidos	Durante os testes não identificamos parâmetros para realização de escalonamento de privilégios.
Tipo de teste executado	Escalação de privilégios

Evidências

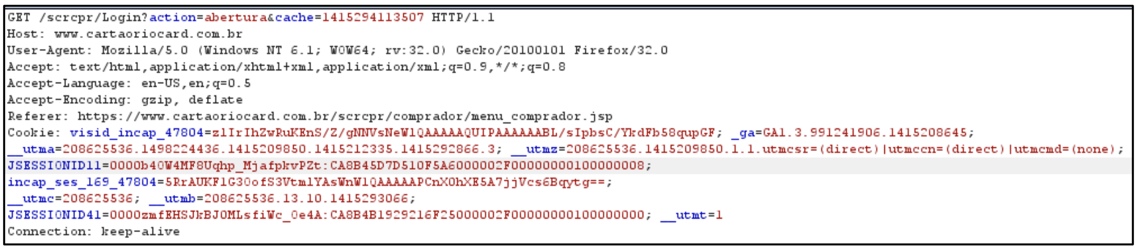


```
POST /scrcpr/Login HTTP/1.1
Host: www.cartaoriocard.com.br
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.cartaoriocard.com.br/scrcpr/geral/frmLogin.jsp
Cookie: visid_incap_47804=zlIrIhZwRuKEnS/Z/gNNVsNeW1QAAAAAQUIPAAAAAABL/sIpbsC/YkdFb58qupGF; _ga=GA1.3.991241906.1415208645; __utma=208625536.1498224436.1415
__utmz=208625536.1415209850.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none); JSESSIONID11=00008Ngt3RYmrTjMezmHSqXnGy-:CA8B45D7D510F5A6000002F000000001000
incap_ses_169_47804=5RrAUKF1G30ofS3VtmlYAsWnW1QAAAAAPCnX0hXE5A7jjVcs6Bqytg==; __utmc=208625536; __utmb=208625536
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 376

nrDoc=johndoe123&senha=Teste1%40&palavraChaveDesafio=03AHJ_Vuu3h-Eedvw7EPt4qQ28IqyaA0aK1HVNqHEoAH1Rm9OYkKvPLAIxJ5JJjqDy9Akao0a3QHCVJyI9W2a9G-dYoBbA5-AZmZC99
3oEgwGn0WSf7sWi8INaL-hbuNAtjCDd04n0DYk16PGVo7KoY-EQoaneKbkuViE6Z38feSD_YWsuoA8I&palavraChaveResposta=called+adeniat&btnEnviar=Entrar&sis=1&loginPage=true
```

6. Manipulação de cookies

Resultados Obtidos	Durante os testes não identificamos informações sensíveis nos cookies de sessão.
Tipo de teste executado	Manipulação de cookies

Evidências

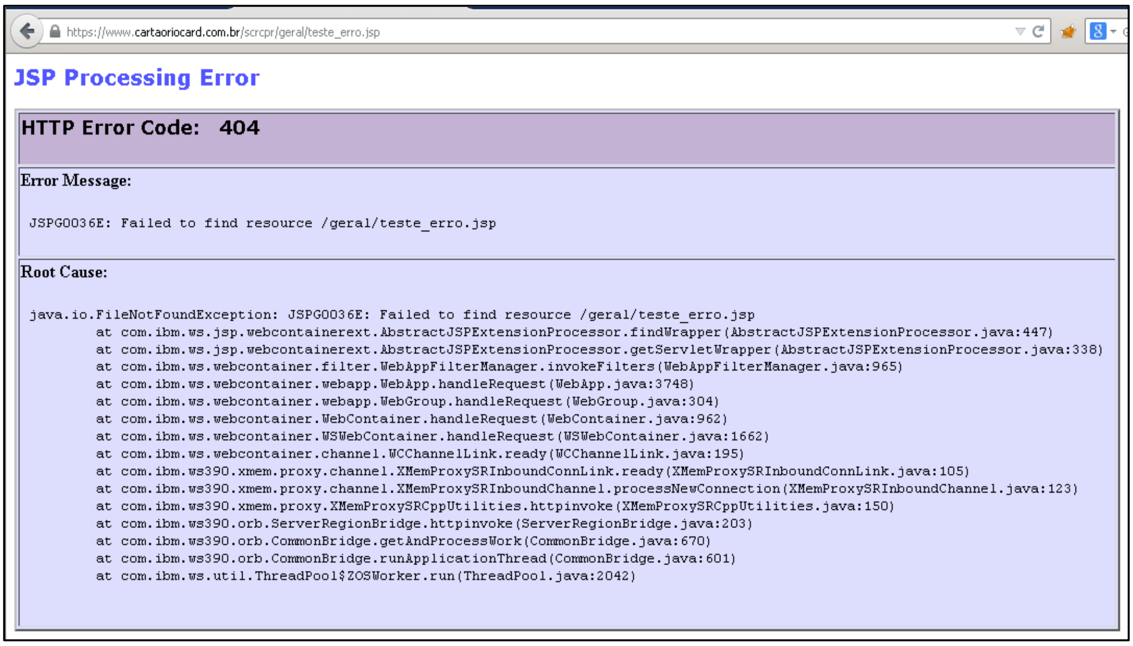


```
GET /scrcpr/Login?action=abertura&cache=1415294113507 HTTP/1.1
Host: www.cartaoriocard.com.br
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:32.0) Gecko/20100101 Firefox/32.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.cartaoriocard.com.br/scrcpr/comprador/menu_comprador.jsp
Cookie: visid_incap_47804=zlIrIhZwRuKEnS/Z/gNNVsNeW1QAAAAAQUIPAAAAAABL/sIpbsC/YkdFb58qupGF; _ga=GA1.3.991241906.1415208645;
__utma=208625536.1498224436.1415209850.1415212335.1415292866.3; __utmz=208625536.1415209850.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
JSESSIONID11=0000b40W4MF8Uqhp_MjafpkvPZt:CA8B45D7D510F5A6000002F000000001000000008;
incap_ses_169_47804=5RrAUKF1G30ofS3VtmlYAsWnW1QAAAAAPCnX0hXE5A7jjVcs6Bqytg==;
__utmc=208625536; __utmb=208625536.13.10.1415293066;
JSESSIONID41=0000zmfEHSJkBJ0MLsfiWc_0e4A:CA8B4B1929216F25000002F000000001000000000; __utmt=1
Connection: keep-alive
```

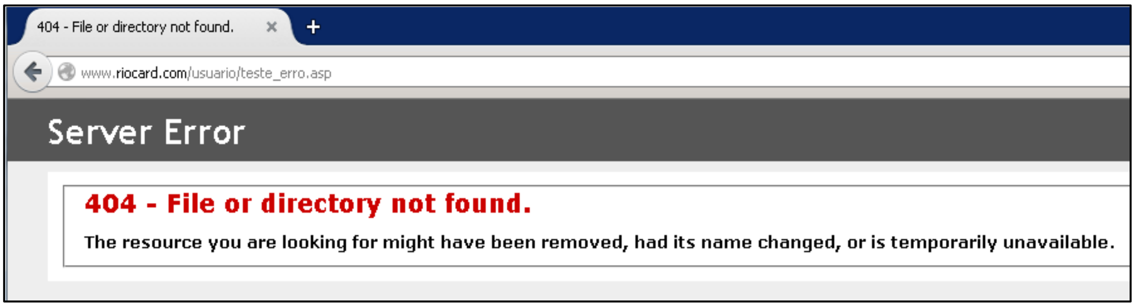
7. Informações de mensagens de erro

Resultado Obtido	Durante os testes forçamos algumas páginas a exibirem mensagens de erro. Identificamos que existem páginas que não possuem tratamento de erro (404, por exemplo), porém não identificamos informações sensíveis como, por exemplo, endereços IP internos, hostnames, etc.
Tipo de teste executado	Utilização de informações em mensagens de erro.

Evidências



```
https://www.cartaoriocard.com.br/scrcpr/geral/teste_erro.jsp

JSP Processing Error

HTTP Error Code:   404

Error Message:

 JSPG0036E: Failed to find resource /geral/teste_erro.jsp

Root Cause:

 java.io.FileNotFoundException: JSPG0036E: Failed to find resource /geral/teste_erro.jsp
        at com.ibm.ws.jsp.webcontainerext.AbstractJSPExtensionProcessor.findWrapper(AbstractJSPExtensionProcessor.java:447)
        at com.ibm.ws.jsp.webcontainerext.AbstractJSPExtensionProcessor.getServletWrapper(AbstractJSPExtensionProcessor.java:338)
        at com.ibm.ws.webcontainer.filter.WebAppFilterManager.invokeFilters(WebAppFilterManager.java:965)
        at com.ibm.ws.webcontainer.webapp.WebApp.handleRequest(WebApp.java:3748)
        at com.ibm.ws.webcontainer.webapp.WebGroup.handleRequest(WebGroup.java:304)
        at com.ibm.ws.webcontainer.WebContainer.handleRequest(WebContainer.java:962)
        at com.ibm.ws.webcontainer.WSWebContainer.handleRequest(WSWebContainer.java:1662)
        at com.ibm.ws.webcontainer.channel.WCChannelLink.ready(WCChannelLink.java:195)
        at com.ibm.ws390.xmem.proxy.channel.XMemProxySRInboundConnLink.ready(XMemProxySRInboundConnLink.java:105)
        at com.ibm.ws390.xmem.proxy.channel.XMemProxySRInboundChannel.processNewConnection(XMemProxySRInboundChannel.java:123)
        at com.ibm.ws390.xmem.proxy.XMemProxySRCppUtilities.httpinvoke(XMemProxySRCppUtilities.java:150)
        at com.ibm.ws390.orb.ServerRegionBridge.httpinvoke(ServerRegionBridge.java:203)
        at com.ibm.ws390.orb.CommonBridge.getAndProcessWork(CommonBridge.java:670)
        at com.ibm.ws390.orb.CommonBridge.runApplicationThread(CommonBridge.java:601)
        at com.ibm.ws.util.ThreadPool$ZOSWorker.run(ThreadPool.java:2042)
```

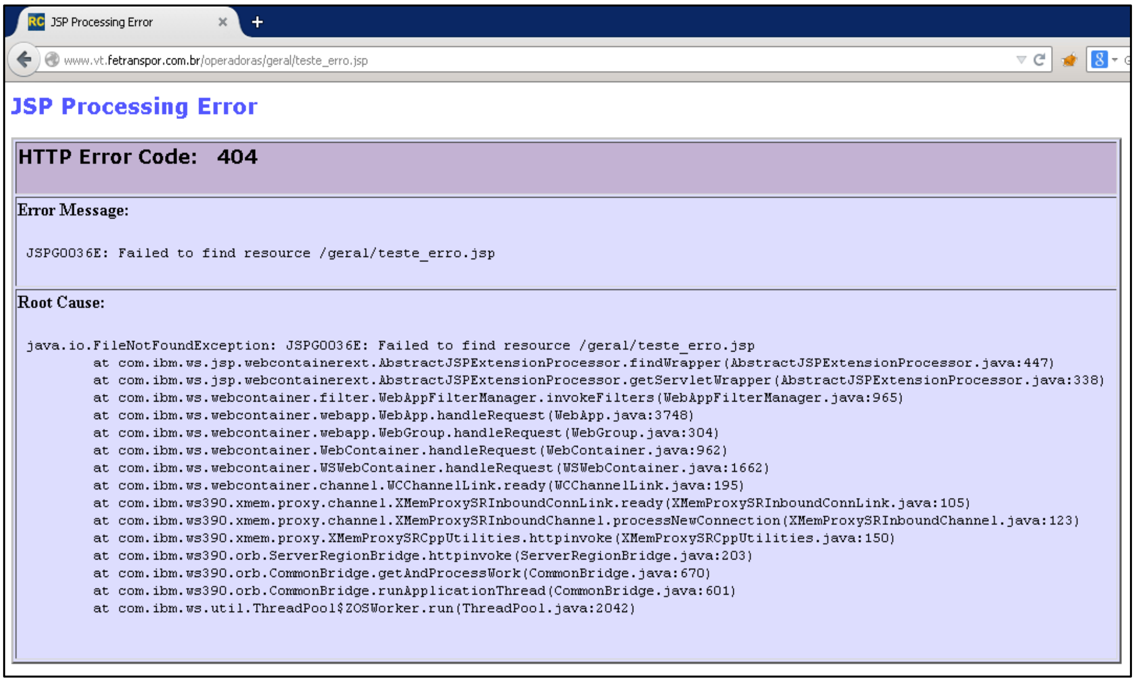


404 - File or directory not found.
www.riocard.com/usuario/teste_erro.asp

Server Error

404 - File or directory not found.

The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.



JSP Processing Error

HTTP Error Code: 404

Error Message:

```
JSPG0036E: Failed to find resource /geral/teste_erro.jsp
```

Root Cause:

```
java.io.FileNotFoundException: JSPG0036E: Failed to find resource /geral/teste_erro.jsp
        at com.ibm.ws.jsp.webcontainerext.AbstractJSPExtensionProcessor.findWrapper(AbstractJSPExtensionProcessor.java:447)
        at com.ibm.ws.jsp.webcontainerext.AbstractJSPExtensionProcessor.getServletWrapper(AbstractJSPExtensionProcessor.java:338)
        at com.ibm.ws.webcontainer.filter.WebAppFilterManager.invokeFilters(WebAppFilterManager.java:965)
        at com.ibm.ws.webcontainer.webapp.WebApp.handleRequest(WebApp.java:3748)
        at com.ibm.ws.webcontainer.webapp.WebGroup.handleRequest(WebGroup.java:304)
        at com.ibm.ws.webcontainer.WebContainer.handleRequest(WebContainer.java:962)
        at com.ibm.ws.webcontainer.WSWebContainer.handleRequest(WSWebContainer.java:1662)
        at com.ibm.ws.webcontainer.channel.WCChannelLink.ready(WCChannelLink.java:195)
        at com.ibm.ws390.xmem.proxy.channel.XMemProxySRInboundConnLink.ready(XMemProxySRInboundConnLink.java:105)
        at com.ibm.ws390.xmem.proxy.channel.XMemProxySRInboundChannel.processNewConnection(XMemProxySRInboundChannel.java:123)
        at com.ibm.ws390.xmem.proxy.XMemProxySRCppUtilities.httpinvoke(XMemProxySRCppUtilities.java:150)
        at com.ibm.ws390.orb.ServerRegionBridge.httpinvoke(ServerRegionBridge.java:203)
        at com.ibm.ws390.orb.CommonBridge.getAndProcessWork(CommonBridge.java:670)
        at com.ibm.ws390.orb.CommonBridge.runApplicationThread(CommonBridge.java:601)
        at com.ibm.ws.util.ThreadPool$ZOSWorker.run(ThreadPool.java:2042)
```

4.1.3.2. Teste de invasão externo de infraestrutura

Durante a execução dos testes, foi identificada a presença de um firewall, que dificultou as ações do atacante, que recebe informações desconectadas como, por exemplo, que todas as portas estão abertas, fechadas ou filtradas.

(a) Varreduras Automatizadas

Para a fase de varredura automatizada, foi utilizada a ferramenta *Nmap*, com o intuito de verificar status de portas e serviços em execução.

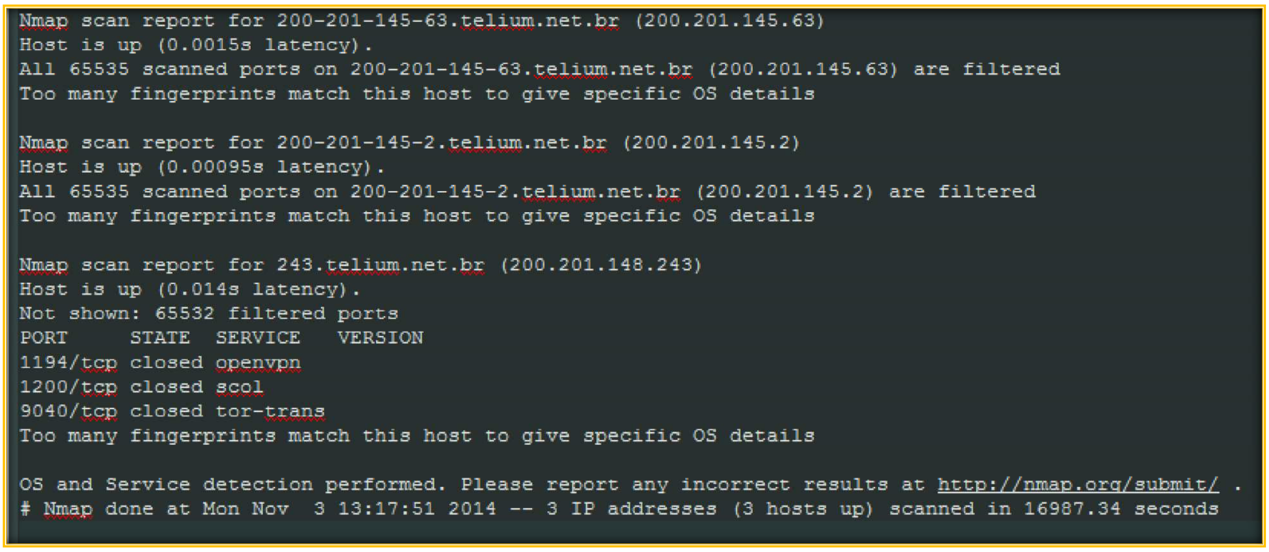
A tabela abaixo exibe o resultado dessa varredura de portas.

IPs	Porta	Protocolo	Status	Serviço
200.201.145.2	-	-	-	-
200.201.148.243	1194	tcp	closed	openvpn
	1200	tcp	closed	scol
	9040	tcp	closed	tor-trans
200.201.145.63	-	-	-	-
199.83.134.73	-	-	-	-
199.83.134.7	-	-	-	-
199.83.134.200	-	-	-	-

Conforme podemos observar na tabela acima, não obtivemos muitos resultados, devido à presença de um firewall à frente dos hosts analisados, que dificultou a realização dessa varredura.

A imagem 1 abaixo mostra que o resultado obtido para os hosts de concentradores de VPN e servidor FTP estão com todas as portas filtradas, exceto um host que exibe três portas fechadas.

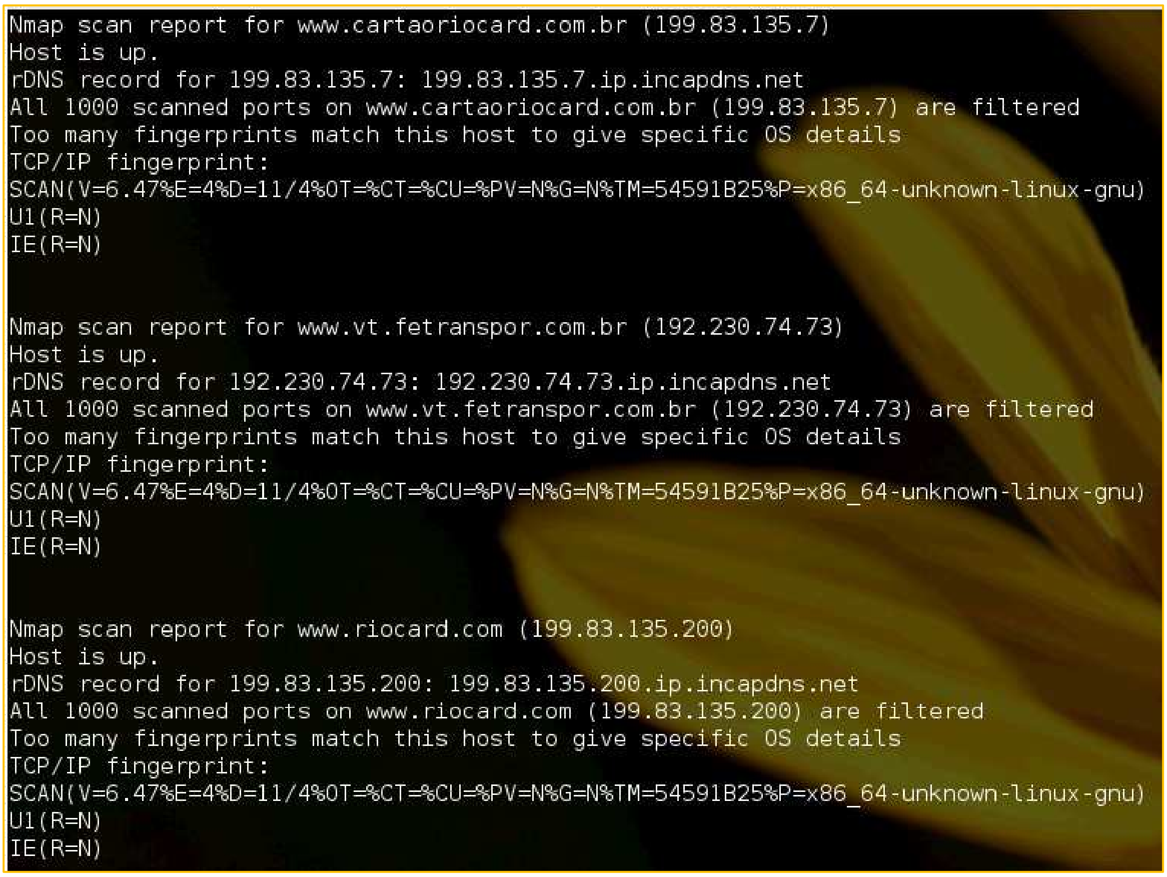
Imagem 1



```
Nmap scan report for 200-201-145-63.telium.net.br (200.201.145.63)
Host is up (0.0015s latency).
All 65535 scanned ports on 200-201-145-63.telium.net.br (200.201.145.63) are filtered
Too many fingerprints match this host to give specific OS details

Nmap scan report for 200-201-145-2.telium.net.br (200.201.145.2)
Host is up (0.00095s latency).
All 65535 scanned ports on 200-201-145-2.telium.net.br (200.201.145.2) are filtered
Too many fingerprints match this host to give specific OS details

Nmap scan report for 243.telium.net.br (200.201.148.243)
Host is up (0.014s latency).
Not shown: 65532 filtered ports
PORT     STATE  SERVICE   VERSION
1194/tcp closed openvpn
1200/tcp closed scol
9040/tcp closed tor-trans
Too many fingerprints match this host to give specific OS details

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
# Nmap done at Mon Nov  3 13:17:51 2014 -- 3 IP addresses (3 hosts up) scanned in 16987.34 seconds
```

Na análise de infraestrutura que suportam os websites, também foi verificado que as portas estão filtradas, conforme mostra a imagem 2.

Imagem 2



```
Nmap scan report for www.cartaoriocard.com.br (199.83.135.7)
Host is up.
rDNS record for 199.83.135.7: 199.83.135.7.ip.incapdns.net
All 1000 scanned ports on www.cartaoriocard.com.br (199.83.135.7) are filtered
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=6.47%E=4%D=11/4%OT=%CT=%CU=%PV=N%G=N%TM=54591B25%P=x86_64-unknown-linux-gnu)
U1(R=N)
IE(R=N)


Nmap scan report for www.vt.fetranspor.com.br (192.230.74.73)
Host is up.
rDNS record for 192.230.74.73: 192.230.74.73.ip.incapdns.net
All 1000 scanned ports on www.vt.fetranspor.com.br (192.230.74.73) are filtered
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=6.47%E=4%D=11/4%OT=%CT=%CU=%PV=N%G=N%TM=54591B25%P=x86_64-unknown-linux-gnu)
U1(R=N)
IE(R=N)


Nmap scan report for www.riocard.com (199.83.135.200)
Host is up.
rDNS record for 199.83.135.200: 199.83.135.200.ip.incapdns.net
All 1000 scanned ports on www.riocard.com (199.83.135.200) are filtered
Too many fingerprints match this host to give specific OS details
TCP/IP fingerprint:
SCAN(V=6.47%E=4%D=11/4%OT=%CT=%CU=%PV=N%G=N%TM=54591B25%P=x86_64-unknown-linux-gnu)
U1(R=N)
IE(R=N)
```

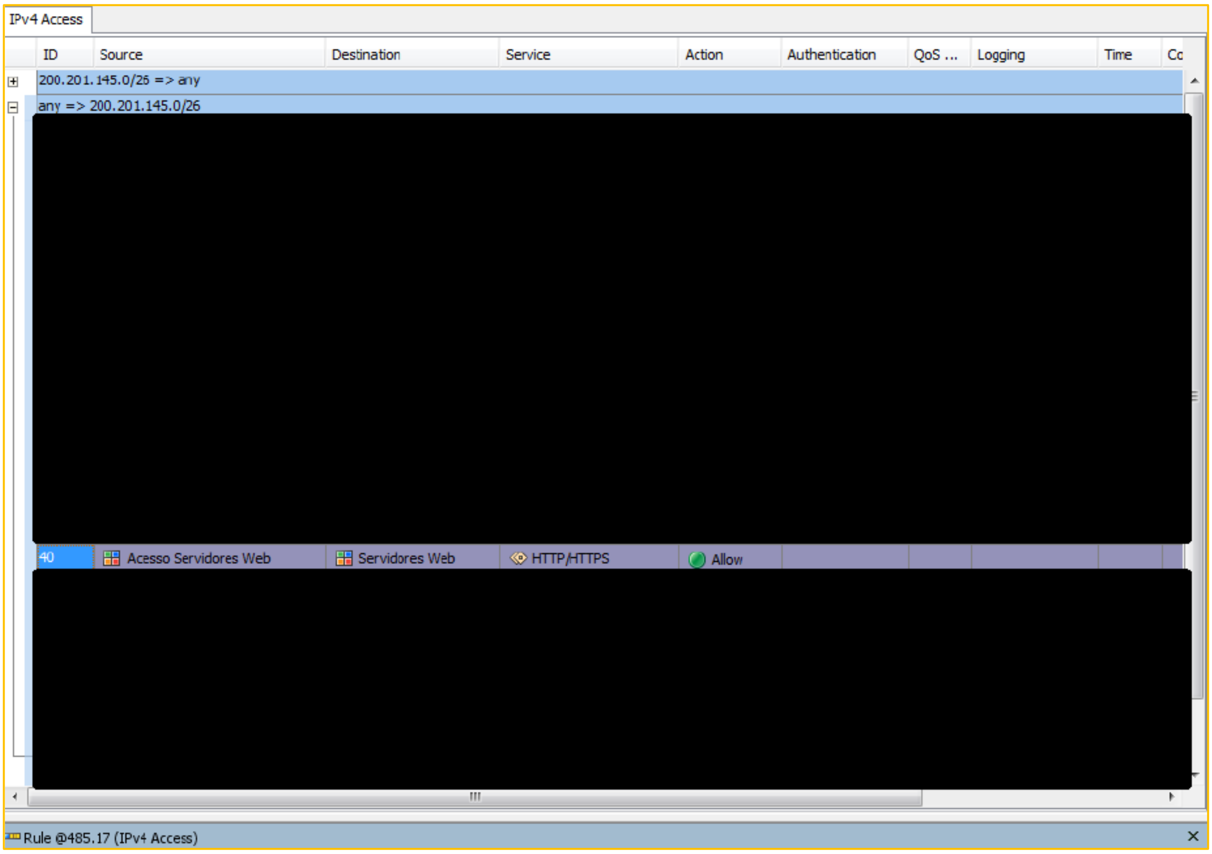
Além da varredura de portas e serviços, executada pela ferramenta Nmap, também foi executada uma varredura automatizada com a ferramenta Nessus.

Abaixo a lista dos grupos de testes que foram realizados com a ferramenta Nessus, totalizando **67.434** testes, cobrindo **27.158 CVEs** e **19.802 Bugtraq Ids**.

1. AIX Local Security Checks
2. Amazon Linux Local Security Checks
3. Backdoors
4. CentOS Local Security Checks
5. CGI abuses
6. CGI abuses : XSS
7. CISCO
8. Databases
9. Debian Local Security Checks
10. Default Unix Accounts
11. Denial of Service
12. DNS
13. F5 Networks Local Security Checks
14. Fedora Local Security Checks
15. Firewalls
16. FreeBSD Local Security Checks
17. FTP
18. Gain a shell remotely
19. General
20. Gentoo Local Security Checks
21. HP-UX Local Security Checks
22. Huawei Local Security Checks
23. Junos Local Security Checks
24. MacOS X Local Security Checks
25. Mandriva Local Security Checks
26. Misc.
27. Mobile Devices
28. Netware
29. Oracle Linux Local Security Checks
30. Palo Alto Local Security Checks
31. Peer-To-Peer File Sharing
32. Policy Compliance
33. Port scanners
34. Red Hat Local Security Checks
35. RPC
36. SCADA
37. Scientific Linux Local Security Checks
38. Service detection
39. Settings
40. Slackware Local Security Checks
41. SMTP problems
42. SNMP
43. Solaris Local Security Checks
44. SuSE Local Security Checks
45. Ubuntu Local Security Checks
46. VMware ESX Local Security Checks
47. Web Servers
48. Windows
49. Windows : Microsoft Bulletins
50. Windows : User manage

Durante a realização dos testes identificamos a existência de um controle de acesso no ambiente de Internet da RioCard, que restringe o acesso apenas pelas portas 80 e 443 (HTTP e HTTPS). Segue abaixo a evidência fornecida:

Imagem 3



IPv4 Access

ID	Source	Destination	Service	Action	Authentication	QoS ...	Logging	Time	Co
200.201.145.0/26 => any									
any => 200.201.145.0/26									
[redacted]									
40	Acesso Servidores Web	Servidores Web	HTTP/HTTPS	Allow					
[redacted]									

Rule @485.17 (IPv4 Access)

4.2. Teste externo de intrusão em ambiente interno

Em conformidade com os parâmetros especificados para a realização dos testes, foi recebida a informação sobre o barramento de rede utilizado pela RioCard o qual suporta as aplicações definidas em escopo do teste externo.

O escopo definido para o início dos trabalhos foram os sistemas que suportam as aplicações definidas no escopo do teste externo, os quais são acessíveis no barramento de rede **10.0.0.0/8**.

Para a realização da execução dos testes utilizamos as seguintes ferramentas: (a) Nessus; (b) Nmap; e (c) Kali Linux.

Conforme descrito anteriormente, durante a execução dos testes foi identificada a presença de controles de segurança que dificultam as ações do atacante, mais especificamente, foi verificada a existência do protocolo de controle de acesso denominado 802.1X o qual controla de forma eficiente o acesso à rede interna da RioCard.

4.2.1. Testes realizados e resultados obtidos

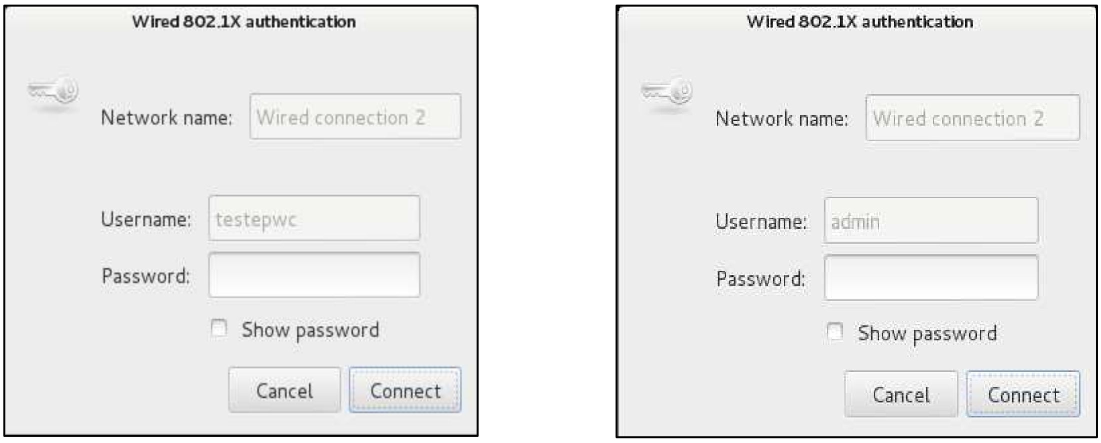
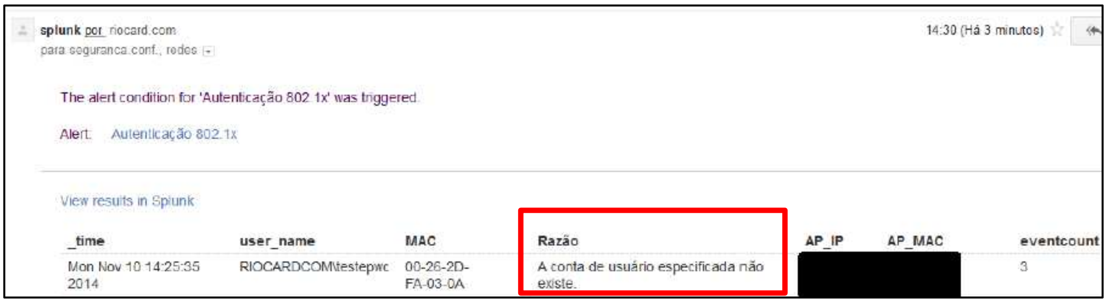
Teste I	
Descrição	Realizar tentativas de autenticação na rede interna da RioCard por meio do protocolo 802.1x. Esse teste cobre o seguinte item do Termo de Referência: (a) *Alert and Log Review*; e (b) *Access Verification*.
Objetivo	Obter acesso à rede interna a partir do ponto de rede disponibilizado na RioCard, situada na Rua da Assembleia, 10, 34º andar, Centro, Rio de Janeiro – RJ.
Resultado	O teste de acesso à rede interna utilizando um ativo não pertencente à RioCard (notebook PwC), demonstrou que o acesso é negado devido ao mecanismo de autenticação para dispositivos que desejam se conectar na rede denominado 802.1X.
Evidências	Adicionalmente, foi realizado teste manual de *brute force*, a fim de obter a autenticação. Na realização desse teste, usuários como "testepwc" e "admin" foram utilizados, e senhas aleatórias foram inseridas. As imagens abaixo mostram a tela exibida para a autenticação 802.1x. **Figura 1**  Wired 802.1X authentication Network name: Wired connection 2 Username: testepwc Password: ☐ Show password Wired 802.1X authentication Network name: Wired connection 2 Username: admin Password: ☐ Show password Durante a execução dos testes de *brute force*, foi gerado um alerta para o time de Segurança e Compliance da RioCard, informando as sucessivas falhas de autenticação, como apresentado a seguir.

Figura 2



splunk por riocard.com
para seguranca.conf., redes

14:30 (Há 3 minutos)

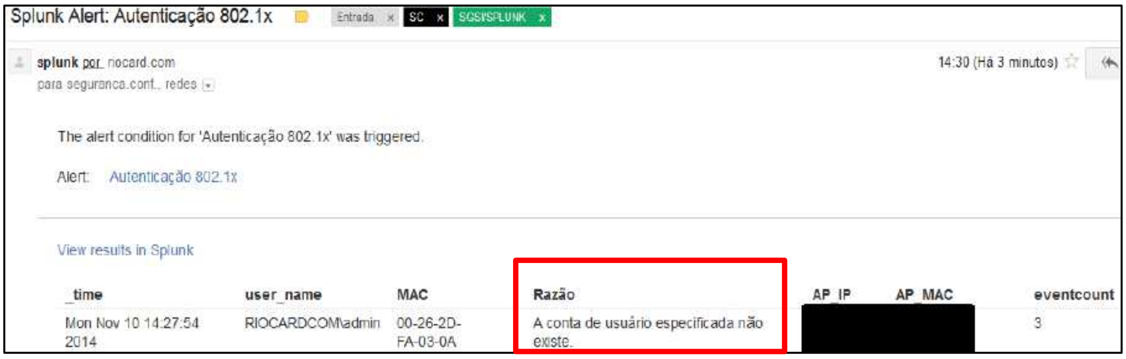
The alert condition for 'Autenticação 802.1x' was triggered.

Alert: Autenticação 802.1x

View results in Splunk

_time	user_name	MAC	Razão	AP_IP	AP_MAC	eventcount
Mon Nov 10 14:25:35 2014	RIOCARDCOM\testepwc	00-26-2D-FA-03-0A	A conta de usuário especificada não existe.	[redacted]	[redacted]	3

Figura 3



Splunk Alert: Autenticação 802.1x

splunk por riocard.com
para seguranca.conf., redes

14:30 (Há 3 minutos)

The alert condition for 'Autenticação 802.1x' was triggered.

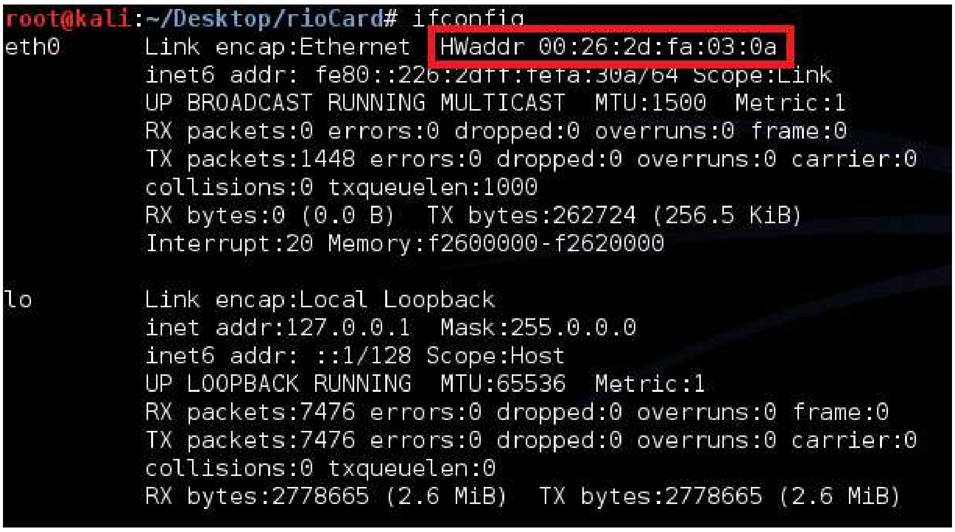
Alert: Autenticação 802.1x

View results in Splunk

_time	user_name	MAC	Razão	AP_IP	AP_MAC	eventcount
Mon Nov 10 14:27:54 2014	RIOCARDCOM\admin	00-26-2D-FA-03-0A	A conta de usuário especificada não existe.	[redacted]	[redacted]	3

Figura 4

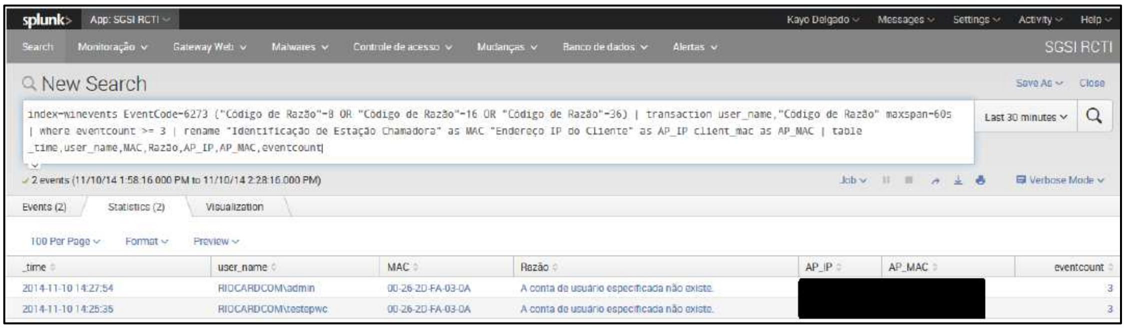
O alerta é detectado pela ferramenta do tipo SIEM (Splunk), que dispara e-mail de notificação para a área de Segurança e Compliance. É possível observar que o “MAC Address” da máquina capturada confere com o utilizado durante os testes. A imagem abaixo mostra o MAC Address do notebook utilizado.



```
root@kali:~/Desktop/rioCard# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:26:2d:fa:03:0a
          inet6 addr: fe80::226:2dff:fefa:30a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1448 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:262724 (256.5 KiB)
          Interrupt:20 Memory:f2600000-f2620000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:7476 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7476 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2778665 (2.6 MiB)  TX bytes:2778665 (2.6 MiB)
```

Figura 5

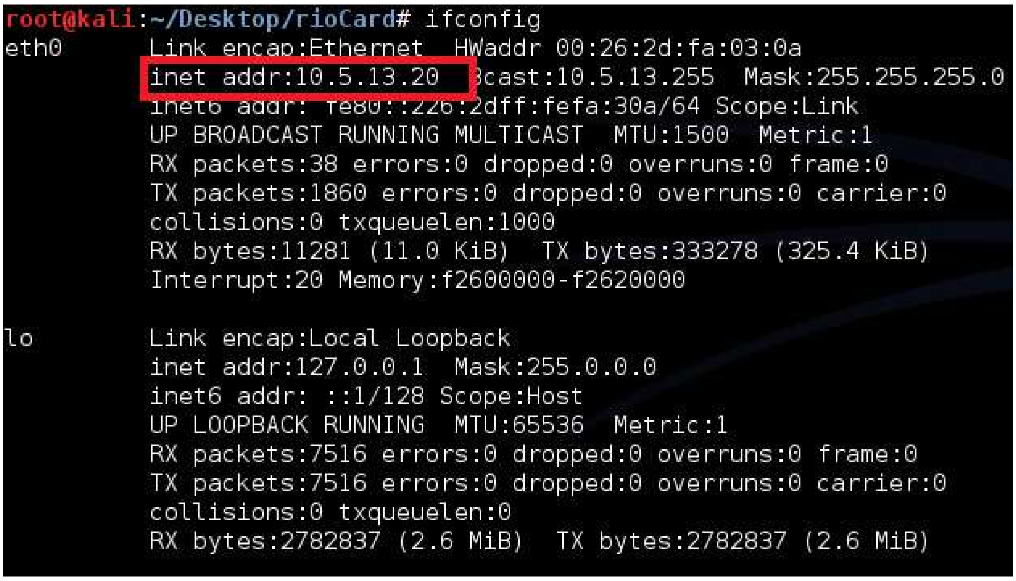
Após o alerta gerado, é iniciado o procedimento de resposta a incidentes que inclui a investigação detalhada do evento, e ações de remediação relacionadas. Através da ferramenta de SIEM é possível visualizar os registros dessas tentativas, conforme apresentado abaixo:


splunk>
App: SGSI RCTI
Kayo Delgado
Messages
Settings
Activity
Help
Search
Monitoração
Gateway Web
Malwares
Controle de acesso
Mudanças
Banco de dados
Alertas
SGSI RCTI
New Search
Save As
Close
Last 30 minutes
Job
Verbose Mode
Events (2)
Statistics (2)
Visualization
100 Per Page
Format
Preview

```
index-winevents EventCode-6273 ("Código de Razão"-8 OR "Código de Razão"-16 OR "Código de Razão"-36) | transaction user_name,"Código de Razão" maxspan-60s
| where eventcount >= 3 | rename "Identificação de Estação Chamadora" as MAC "Endereço IP do Cliente" as AP_IP client_mac as AP_MAC | table
_time,user_name,MAC,Razão,AP_IP,AP_MAC,eventcount
```

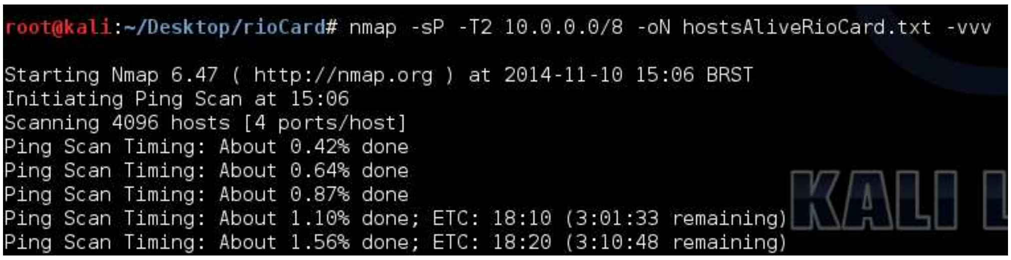
2 events (11/10/14 1:58:16.000 PM to 11/10/14 2:28:16.000 PM)

_time	user_name	MAC	Razão	AP_IP	AP_MAC	eventcount
2014-11-10 14:27:54	RIOCARDCOM\admin	00-26-2D-FA-03-0A	A conta de usuário especificada não existe.	[redacted]	[redacted]	3
2014-11-10 14:25:35	RIOCARDCOM\testepwc	00-26-2D-FA-03-0A	A conta de usuário especificada não existe.	[redacted]	[redacted]	3

Teste II	
Descrição	Varredura automatizada de *hosts* ativos com a ferramenta *Nmap*. Esse teste cobre os seguintes itens do Termo de Referência: (a) *Visibility Audit*; e (b) *Alert and Log Review*.
Objetivo	Levantar informações e identificar *hosts* ativos na rede interna previamente ao mapeamento de portas de comunicação.
Resultado	Para a realização deste teste, acesso à rede da RioCard foi necessária e, portanto, uma credencial foi criada pela área de Segurança e Compliance. A credencial criada para os testes foi "joao.pwc" com senha inicial de 8 (oito) caracteres. Em posse da credencial, foi possível obter um endereço IP na rede local da RioCard. É importante salientar que o usuário "joao.pwc" foi disponibilizado exclusivamente para a realização deste teste.
Evidências	**Figura 1 – Endereço IP obtido**  **Figura 2** Para realizar a varredura automatizada, foi utilizada a ferramenta Nmap. Primeiramente, foi executado o seguinte comando: "*nmap –sP –T2 10.0.0.0/8 -oN hostsAliveRioCard.txt –vvv*". Esse comando tem como objetivo levantar os endereços IP ativos. A imagem abaixo mostra essa varredura durante execução.

Evidências – Figura 1:

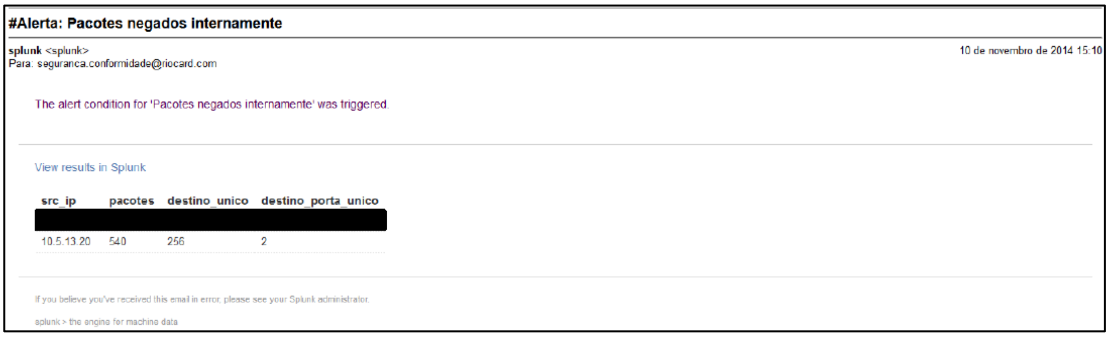
```
root@kali:~/Desktop/rioCard# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:26:2d:fa:03:0a
          inet addr:10.5.13.20  Bcast:10.5.13.255  Mask:255.255.255.0
          inet6 addr: fe80::226:2dff:fefa:30a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1860 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11281 (11.0 KiB)  TX bytes:333278 (325.4 KiB)
          Interrupt:20 Memory:f2600000-f2620000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:7516 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7516 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2782837 (2.6 MiB)  TX bytes:2782837 (2.6 MiB)
```



```
root@kali:~/Desktop/rioCard# nmap -sP -T2 10.0.0.0/8 -oN hostsAliveRioCard.txt -vvv

Starting Nmap 6.47 ( http://nmap.org ) at 2014-11-10 15:06 BRST
Initiating Ping Scan at 15:06
Scanning 4096 hosts [4 ports/host]
Ping Scan Timing: About 0.42% done
Ping Scan Timing: About 0.64% done
Ping Scan Timing: About 0.87% done
Ping Scan Timing: About 1.10% done; ETC: 18:10 (3:01:33 remaining)
Ping Scan Timing: About 1.56% done; ETC: 18:20 (3:10:48 remaining)
```

Figura 3

Entretanto, durante a execução desse teste, alertas adicionais foram gerados para o time de Segurança e Compliance, conforme mostra a figura a seguir.



#Alerta: Pacotes negados internamente

splunk <splunk>
Para: seguranca.conformidade@riocard.com
10 de novembro de 2014 15:10

The alert condition for 'Pacotes negados internamente' was triggered.

View results in Splunk

src_ip	pacotes	destino_unico	destino_porta_unico
[redacted]	[redacted]	[redacted]	[redacted]
10.5.13.20	540	256	2

If you believe you've received this email in error, please see your Splunk administrator.

splunk > the engine for machine data

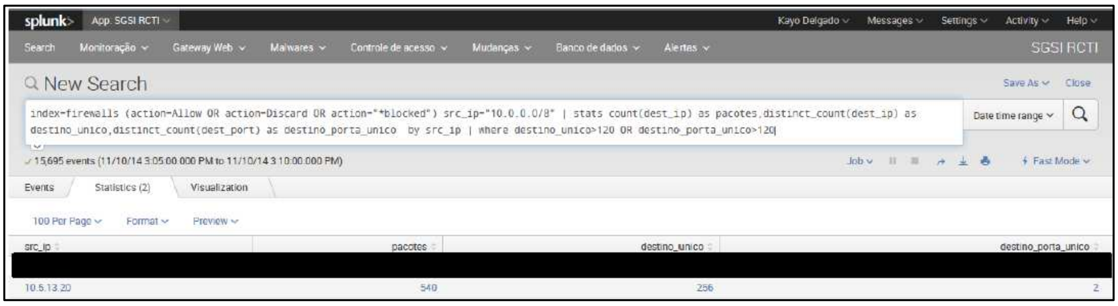
Figura 4

Podemos verificar que, nesse e-mail, consta o endereço IP da máquina de teste.

Após a geração do alerta, o time de Segurança e Compliance inicia o procedimento de resposta a incidentes para averiguar o evento ocorrido.

Os *logs* gerados são analisados na ferramenta de SIEM e, subsequentemente, mediante solicitação da RioCard a varredura foi abortada.

A imagem abaixo exibe o registro desse evento ocorrido durante os testes.

splunk>
App: SGSI RCTI
Kayo Delgado
Messages
Settings
Activity
Help
Search
Monitoração
Gateway Web
Malwares
Controle de acesso
Mudanças
Banco de dados
Alertas
SGSI RCTI
New Search
Save As
Close
Date time range
Job
Fast Mode
Events
Statistics (2)
Visualization
100 Per Page
Format
Preview

```
index-firewalls (action-Allow OR action-Discard OR action-"*blocked") src_ip-"10.0.0.0/8" | stats count(dest_ip) as pacotes,distinct_count(dest_ip) as
destino_unico,distinct_count(dest_port) as destino_porta_unico  by src_ip | where destino_unico>120 OR destino_porta_unico>120
```

✓ 15,695 events (11/10/14 3:05:00.000 PM to 11/10/14 3:10:00.000 PM)

src_ip	pacotes	destino_unico	destino_porta_unico
[redacted]	[redacted]	[redacted]	[redacted]
10.5.13.20	540	256	2

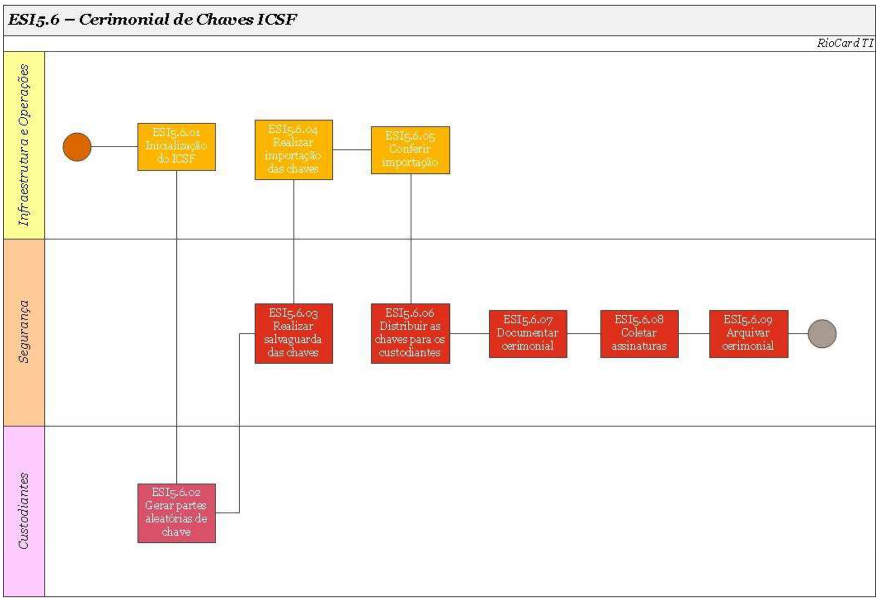
Teste III	
Descrição	Utilizar uma ferramenta de *sniffing* de rede para monitorar os pacotes de comunicação de rede com os servidores das aplicações. Esse teste cobre o item de *Visibility Audit* do Termo de Referência.
Objetivo	Levantar endereços IP válidos para realizar testes direcionados.
Resultados	Não foi realizado devido a não obtenção de acesso a rede interna conforme descrito no resultado do Teste II.
Evidências	Não Aplicável
Teste IV	
Descrição	Realizar simulação de ataque com a técnica de *ARP Poisoning e MAC Spoofing*. Esse teste cobre o item *Trust Verification* do Termo de Referência.
Objetivo	Obter um MAC Address de um ativo conectado à rede (Ex.: Impressora) e atribuí-lo à máquina de teste, a fim de obter acesso à rede.
Resultado	Não foi realizado devido ao risco de indisponibilidade de ativos.
Evidências	Não Aplicável

Teste V	
Descrição	Realizar a varredura de portas e serviços utilizando a ferramenta Nmap. Esse teste cobre os seguintes itens do Termo de Referência: (a) *Access Verification*; (b) *Visibility Audit*; (c) *Access Verification*; (d) *Active Detection Verification*; (e) *Controls Verification*; (f) *Process Verification*; (g) *Configuration Verification*; (h) *Property Validation*; (i) *Exposure Verification*; e (j) *Privileges Audit*.
Objetivo	Mapear o *status* das portas e serviços em execução nos *hosts* ativos na rede da RioCard a fim de identificar possíveis vetores de ataque.
Resultado	Não foi realizado devido a não obtenção de acesso a rede interna conforme descrito no resultado do Teste II.
Evidências	Não Aplicável
Teste VI	
Descrição	Realizar testes manuais em portas e serviços.
Objetivo	Com o resultado obtido no Teste V, validar manualmente as portas e serviços identificados a fim de verificar possíveis vulnerabilidades.
Resultado	Não foi realizado, devido a não realização do teste V.
Evidencias	Não Aplicável
Teste VII	
Descrição	Realizar a varredura automatizada de vulnerabilidades com a ferramenta Nesus, a qual realiza um total 67.434 testes, cobrindo 27.158 CVEs e 19.802 Bugtraq Ids. Esse teste cobre os seguintes itens do Termo de Referência: *(a) Logistics; (b) Active Detection Verification; (c) Visibility Audit; (d) Access Verification; (e) Trust Verification; (f) Controls Verification; (g) Process Verification; (h) Configuration Verification; (i) Property Validation; (j) Segregation Review; (k) Exposure Verification; (l) Competitive Intelligence Scouting; (m) Quarantine Verification; (n) Privileges Audit; e (o) Survivability Validation.*
Objetivo	Identificar vulnerabilidades nos *hosts* ativos na rede da RioCard, a fim de verificar oportunidades de melhoria no ambiente tecnológico.
Resultado	Não foi realizado, devido a impossibilidade de realização do teste VI.
Evidências	Não Aplicável

Teste VIII	
Descrição	Exploração de vulnerabilidades.
Objetivo	Validar as vulnerabilidades identificadas na varredura automatizada do Teste VII.
Resultado	Não foi realizado, devido a impossibilidade de realização do teste VII.
Evidências	Não Aplicável

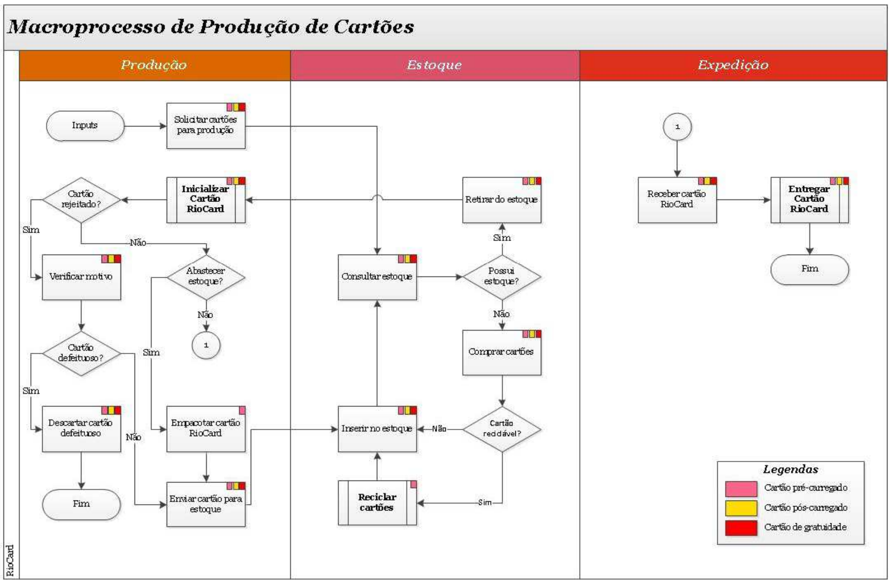
Anexo A – Fluxograma do processo de geração das chaves

O fluxo abaixo descreve o processo da geração e distribuição das chaves criptográficas, desde a inicialização do ICSF (IBM *Cryptography System Facility*) em branco até a coleta de assinaturas e arquivamento do cerimonial.


ESI5.6 – Cerimonial de Chaves ICSF
RioCard TI
Infraestrutura e Operações
Segurança
Custodiantes
ESI5.6.01 Inicialização do ICSF
ESI5.6.02 Gerar partes aleatórias de chave
ESI5.6.03 Realizar salvaguarda das chaves
ESI5.6.04 Realizar importação das chaves
ESI5.6.05 Conferir importação
ESI5.6.06 Distribuir as chaves para os custodiantes
ESI5.6.07 Documentar cerimonial
ESI5.6.08 Coletar assinaturas
ESI5.6.09 Arquivar cerimonial

Anexo B – Fluxograma do processo de fabricação de cartões

O fluxo abaixo descreve o processo de produção dos cartões utilizados no Sistema de Bilhetagem Eletrônica emitidos pela RioCard.


Macroprocesso de Produção de Cartões
Produção
Estoque
Expedição
RioCard
Inputs
Solicitar cartões para produção
Inicializar Cartão RioCard
Cartão rejeitado?
Sim
Não
Verificar motivo
Abastecer estoque?
Não
1
Sim
Cartão defeituoso?
Sim
Não
Descartar cartão defeituoso
Empacotar cartão RioCard
Enviar cartão para estoque
Fim
Retirar do estoque
Sim
Consultar estoque
Possui estoque?
Não
Comprar cartões
Cartão reciclável?
Não
Sim
Inserir no estoque
Reciclar cartões
1
Receber cartão RioCard
Entregar Cartão RioCard
Fim
Legendas
🟥 Cartão pré-carregado
🟨 Cartão pós-carregado
🟥 Cartão de gratuidade

Anexo C – Matriz de Vulnerabilidades de Aplicação Web

#	URL	Caminho	Vulnerabilidade	Descrição	Severidade	Recomendação
1	http://www.riocard.com	/usuario/petropolis_cad_senior/senior/detalhe_apoio.asp	Failure to Restrict URL Access	Foram identificadas aplicações web que realizam a checagem de permissões antes da geração das proteções de botões e links. Entretanto, como as aplicações não realizam o controle de permissões toda vez que a página for acessada, foi possível acessar e alterar as informações presentes nas páginas sem a utilização de credenciais.	Crítico	É recomendável que se use restrição de permissão (ACLS) para impossibilitar leitura anônima dos arquivos/pastas e também para não permitir o acesso e alteração a informações restritas da aplicação web.
2	http://www.vt.fetranspor.com.br/operadoras	Web Server	Cleartext submission of password	Senhas estão sendo transmitidas através de um canal não criptografado. Um usuário malicioso pode interceptar as senhas por esse canal. Este tipo de informação deve ser transferido sempre por canais criptografados (HTTPS) para evitar a interceptação das informações por usuários maliciosos.	Alto	É recomendável que as informações sensíveis sejam trafegadas por conexões criptografadas (HTTPS) para que os dados não sejam interceptados por um usuário malicioso.
3	http://www.riocard.com	Web Server	Cleartext submission of password	Senhas estão sendo transmitidas através de um canal não criptografado. Um usuário malicioso pode interceptar as senhas por esse canal. Este tipo de informação deve ser transferido sempre por canais criptografados (HTTPS) para evitar a	Alto	É recomendável que as informações sensíveis sejam trafegadas por conexões criptografadas (HTTPS) para que os dados não sejam interceptados por um usuário malicioso.

#	URL	Caminho	Vulnerabilidade	Descrição	Severidade	Recomendação
				interceptação das informações por usuários maliciosos.		
4	http://www.riocard.com	/images /noticias /Scripts /style /swf /usuario	Directory Listing	O web server se encontra configurado para mostrar a lista de arquivos contidos em seus diretórios, dentre esses arquivos podem estar contidos diversas informações que podem ser confidenciais ou podem ser utilizadas para gerar um ataque mais sofisticado a esse servidor.	Médio	É recomendado a avaliação da necessidade de se ter a possibilidade de se listar arquivos e de garantir de que esses arquivos não exponham informações que possam ser utilizadas por usuários mal intencionados. Recomendamos que não seja habilitada a possibilidade de listagem de diretórios nas configurações do web server.
5	http://www.riocard.com	/ /cadrdv /cadrdv/login/esqueciminhasenha.asp /usuario/identificausuario.asp	HTML form without CSRF protection	Cross-site request forgery (falsificação de requisição através de site) é um ataque que explora a confiança em usuários dos sites, forjando uma requisição de um usuário de confiança do site para rodar scripts forçando um usuário a executar comandos da escolha do usuário mal intencionado. Um ataque que obtém sucesso pode comprometer os dados ou a operação de usuários finais. Caso o alvo seja um usuário administrador toda a aplicação pode ser comprometida.	Médio	É recomendado utilizar como medida de prevenção a implementação e inclusão de *tokens* na sessão (atual) de um usuário. *Tokens* são valores criptográficos longos que são difíceis de adivinhar. *Tokens* serão gerados quando a sessão de um usuário começar e será associada com a sessão deste usuário em particular. Esse *challange token* será incluído em cada solicitação, que será usado pelo lado do servidor para verificar a legitimidade da requisição do usuário final.

#	URL	Caminho	Vulnerabilidade	Descrição	Severidade	Recomendação
6	http://www.riocard.com	http://www.riocard.com/secimg/seg.asp	CAPTCHA Validation in the Client Side	Código do Captcha está facilmente acessível no código HTML da página, podendo ser explorado por ferramentas automatizadas.	Médio	É recomendado que a verificação do CAPTCHA deva ser feito no servidor sem ser exposto ao lado cliente da comunicação.
7	https://www.cartaoriocard.com.br	Web Server	TLS1/SSLv3 Renegotiation Vulnerability	Uma vulnerabilidadenoss protocolos SSL e TLS permite pedidos de renegociação que pode permitir a invasor injetar texto simples em um stream de protocolo de aplicação. Isso poderia resultar numa situação em que o atacante pode ser capaz de emitir comandos para o servidor que parecem estar vindo de uma fonte legítima. Esse problema afeta SSL versão 3.0 e mais recentes e TLS versão 1.0 e mais recentes.	Médio	A causa da vulnerabilidade pode depender de aplicação para aplicação, uma análise mais profunda deve ser realizada para a correção do problema. É recomendável entrar em contato com o responsável pela aplicação para a correção do problema.
8	https://www.cartaoriocard.com.br	/scrcpr/FaleConosco /vt/visitante/consultas/CarregarCidades.do /vt/visitante/consultas/consultacpf.jsp /vt/visitante/consultas/MostrarRecargasCartoes.do /vt/visitante/home	HTML form without CSRF protection	Cross-site request forgery (falsificação de requisição através de site) é um ataque que explora a confiança em usuários dos sites, forjando uma requisição de um usuário de confiança do site para rodar scripts forçando um usuário a executar comandos da escolha do usuário mal intencionado. Um ataque que obtém sucesso pode comprometer os dados ou a operação de usuários finais. Caso o alvo seja um usuário administrador toda a aplicação pode ser	Médio	É recomendado utilizar como medida de prevenção a implementação e inclusão de *tokens* na sessão (atual) de um usuário. *Tokens* são valores criptográficos longos que são difíceis de adivinhar. *Tokens* serão gerados quando a sessão de um usuário começar e será associada com a sessão deste usuário em particular. Esse *challange token* será incluído em cada solicitação, que será usado

#	URL	Caminho	Vulnerabilidade	Descrição	Severidade	Recomendação
				comprometida.		pelo lado do servidor para verificar a legitimidade da requisição do usuário final.
9	http://www.vt.fetranspor.com.br/operadoras	Web Server	Clickjacking: X-Frame-Options header missing	Clickjacking é uma técnica utilizada por atacantes para enganar usuários comuns a clicarem em links ou objetos maliciosos, ou até mesmo, alterar os links genuínos por esses objetos. Essa técnica pode levar ao vazamento de informações confidenciais ou até mesmo levar ao controle do computador do usuário enquanto o mesmo clica em páginas web aparentemente inócuas. O servidor não retornou um cabeçalho X-frame-Options. Isto significa que este site pode estar em risco de um ataque de clickjacking. O cabeçalho de resposta HTTP X-Frame-Options pode ser usada para indicar ou não se um navegador deve ser autorizado a renderizar uma página em um <frame> ou <iframe>. Os sites podem usar isso para evitar ataques clickjacking, assegurando que o seu conteúdo não é incorporado outros sites.	Baixo	É recomendado configurar seu servidor web para incluir um cabeçalho X-frame-Options.

#	URL	Caminho	Vulnerabilidade	Descrição	Severidade	Recomendação
10	http://www.vt.fetranspor.com.br/operadoras	Web Server	OPTIONS method is enabled	O método HTTP OPTIONS está habilitado para este web server. Este método fornece uma lista de métodos que são suportados pelo web server apresentando uma lista de opções de comunicação disponíveis nas requisições e respostas aceitas pela Request-URI. Informações sensíveis sobre o funcionamento do web server podem ser expostas a usuários maliciosos, apresentando vetores de ataques mais avançados.	Baixo	É recomendável se desabilitar todos os métodos não necessários e de desenvolvimento para sites de produção.
11	http://www.vt.fetranspor.com.br/operadoras	Web Server	Session Cookie without HttpOnly flag set	A sinalização HTTPOnly instrui o navegador de que os cookies só podem ser acessados pelo servidor, se tornando inacessíveis pelo navegador do client. Essa sinalização é uma medida de segurança para proteção de cookies de sessão e autenticação, quando não configurada, os usuários mal intencionados podem utilizar esses cookies para executar ataques, roubar contas de usuários ou realizar scans automatizado em zonas autenticadas.	Baixo	É recomendável verificar a possibilidade de se habilitar o HTTPOnly para aprimorar a proteção dos cookies de sessão de sua aplicação.

#	URL	Caminho	Vulnerabilidade	Descrição	Severidade	Recomendação
12	http://www.vt.fetranspor.com.br/operadoras	Web Server	Session Cookie without Secure flag set	A sinalização de segurança (*Secure flag*) do Cookie não está configurada. Essa sinalização no Cookie indica ao navegador que o Cookie só pode ser acessado através de canais seguros SSL. Essa configuração é importante para se proteger os Cookies de Sessão de uma aplicação.	Baixo	É recomendado colocar a *Secure flag* para esse cookie.
13	http://www.riocard.com	Web Server	Clickjacking: X-Frame-Options header missing	Clickjacking é uma técnica utilizada por atacantes para enganar usuários comuns a clicarem em links ou objetos maliciosos, ou até mesmo, alterar os links genuínos por esses objetos. Essa técnica pode levar ao vazamento de informações confidenciais ou até mesmo levar ao controle do computador do usuário enquanto o mesmo clica em páginas web aparentemente inócuas. O servidor não retornou um cabeçalho X-frame-Options. Isto significa que este site pode estar em risco de um ataque de clickjacking. O cabeçalho de resposta HTTP X-Frame-Options pode ser usada para indicar ou não se um navegador deve ser autorizado a renderizar uma página em um <frame> ou <iframe>. Os sites podem usar isso para evitar ataques	Baixo	É recomendado configurar seu servidor web para incluir um cabeçalho X-frame-Options.

#	URL	Caminho	Vulnerabilidade	Descrição	Severidade	Recomendação
				clickjacking, assegurando que o seu conteúdo não é incorporado outros sites.		
14	http://www.riocard.com	Web Server	OPTIONS method is enabled	O método HTTP OPTIONS está habilitado para este web server. Este método fornece uma lista de métodos que são suportados pelo web server apresentando uma lista de opções de comunicação disponíveis nas requisições e respostas aceitas pela Request-URI. Informações sensíveis sobre o funcionamento do web server podem ser expostas a usuários maliciosos, apresentando vetores de ataques mais avançados.	Baixo	É recomendável se desabilitar todos os métodos não necessários e de desenvolvimento para sites de produção.
15	http://www.riocard.com	Web Server	Session Cookie without HttpOnly flag set	A sinalização HTTPOnly instrui o navegador de que os cookies só podem ser acessados pelo servidor, se tornando inacessíveis pelo navegador do client. Essa sinalização é uma medida de segurança para proteção de cookies de sessão e autenticação, quando não configurada, os usuários mal intencionados podem utilizar esses cookies para executar ataques, roubar contas de usuários ou realizar scans automatizado em zonas autenticadas.	Baixo	É recomendável verificar a possibilidade de se habilitar o HTTPOnly para aprimorar a proteção dos cookies de sessão de sua aplicação.

#	URL	Caminho	Vulnerabilidade	Descrição	Severidade	Recomendação
16	http://www.riocard.com	Web Server	Session Cookie without Secure flag set	A sinalização de segurança (*Secure flag*) do Cookie não está configurada. Essa sinalização no Cookie indica ao navegador que o Cookie só pode ser acessado através de canais seguros SSL. Essa configuração é importante para se proteger os Cookies de Sessão de uma aplicação.	Baixo	É recomendado colocar a *Secure flag* para esse cookie
17	https://www.cartaoriocard.com.br	Web Server	Clickjacking: X-Frame-Options header missing	Clickjacking é uma técnica utilizada por atacantes para enganar usuários comuns a clicarem em links ou objetos maliciosos, ou até mesmo, alterar os links genuínos por esses objetos. Essa técnica pode levar ao vazamento de informações confidenciais ou até mesmo levar ao controle do computador do usuário enquanto o mesmo clica em páginas web aparentemente inócuas. O servidor não retornou um cabeçalho X-frame-Options. Isto significa que este site pode estar em risco de um ataque de clickjacking. O cabeçalho de resposta HTTP X-Frame-Options pode ser usada para indicar ou não se um navegador deve ser autorizado a renderizar uma página em um <frame> ou <iframe>. Os sites	Baixo	É recomendado configurar seu servidor web para incluir um cabeçalho X-frame-Options.

#	URL	Caminho	Vulnerabilidade	Descrição	Severidade	Recomendação
				podem usar isso para evitar ataques clickjacking, assegurando que o seu conteúdo não é incorporado outros sites.		
18	https://www.cartaoriocard.com.br	Web Server	OPTIONS method is enabled	O método HTTP OPTIONS está habilitado para este web server. Este método fornece uma lista de métodos que são suportados pelo web server apresentando uma lista de opções de comunicação disponíveis nas requisições e respostas aceitas pela Request-URI. Informações sensíveis sobre o funcionamento do web server podem ser expostas a usuários maliciosos, apresentando vetores de ataques mais avançados.	Baixo	É recomendável se desabilitar todos os métodos não necessários e de desenvolvimento para sites de produção.

Anexo D – Matriz de Vulnerabilidades de Infraestrutura

Nota: Durante as varreduras automatizadas foram encontradas vulnerabilidades de SSL de severidade média e baixa nas seguintes portas:

- *443*
- *446*
- *7002*
- *7004*
- *8000*
- *8002*
- *8082*
- *8443*
- *8444*
- *8445*
- *10000*
- *50000*

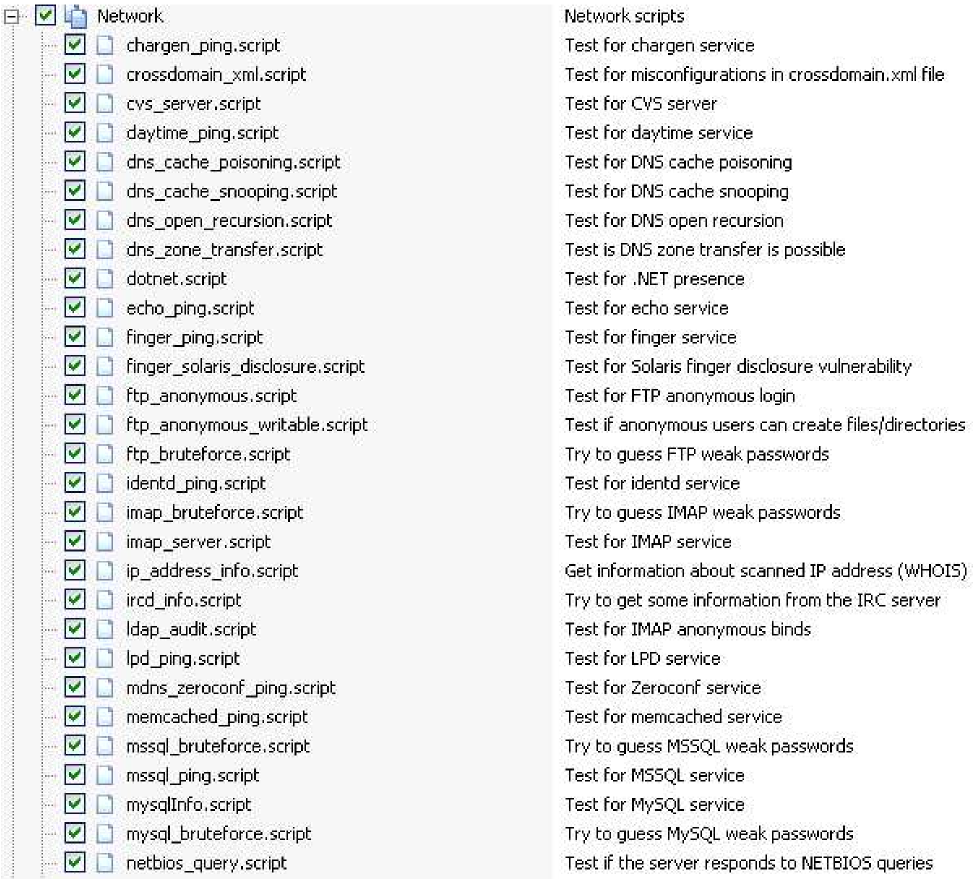
Entretanto, como evidenciado na seção "Teste de invasão externo de infraestrutura", devido ao controle de acesso presente que permite o acesso pela Internet apenas através das portas 80 e 443 (HTTP e HTTPS), foram consideradas apenas as vulnerabilidades referentes a porta 443/tcp para os IPs 199.83.135.200, 192.230.74.73, conforme listadas na tabela a seguir:

#	IP	Porta(s)	Vulnerabilidade	Descrição	Severidade	Recomendação
1	200.201.145.2	500/tcp	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	O serviço remoto Internet Key Exchange (IKE) versão 1 parece suportar o modo agressivo com autenticação PSK. Tal configuração pode permitir que um invasor capture e acesse o PSK de um gateway VPN e ganhe acesso não autorizado para as redes privadas.	Médio	– Desativar o Modo Agressivo, se suportado. – Não usar chave pré-compartilhada para autenticação, se possível. – Se estiver usando chave pré-compartilhada, usar senhas fortes. – Se possível, não permita conexões VPN para certos endereços IP.
2	199.83.135.200	443/tcp	SSL Certificate Cannot Be Trusted	O certificado X.509 não está assinado por uma autoridade certificadora conhecida. Se o host remoto está em produção poderá ocorrer a anulação do uso de SSL e alguém poderia utilizar um ataque de Man in the Middle contra o host.	Médio	É recomendado avaliar se é necessário instalar um novo certificado assinado por uma autoridade certificadora.

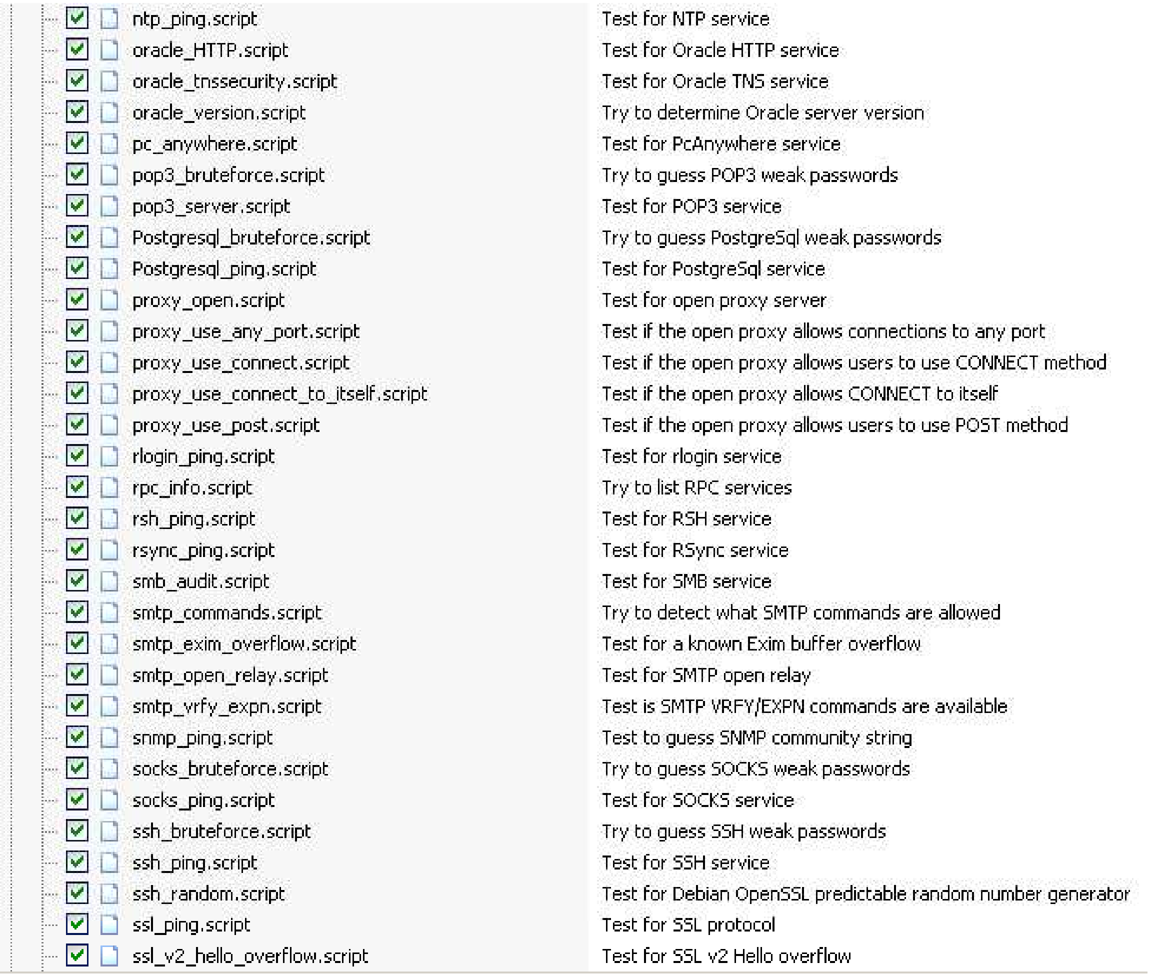
#	IP	Porta(s)	Vulnerabilidade	Descrição	Severidade	Recomendação
3	192.230.74.73	443/tcp	SSL Certificate Cannot Be Trusted	O certificado X.509 não está assinado por uma autoridade certificadora conhecida. Se o host remoto está em produção poderá ocorrer a anulação do uso de SSL e alguém poderia utilizar um ataque de Man in the Middle contra o host.	Médio	É recomendado avaliar se é necessário instalar um novo certificado assinado por uma autoridade certificadora.
4	200.201.148.243	N/A	Disclosure of Personal Information	Informações sobre contatos e endereços de email com domínio não corporativo puderam ser identificadas através de consultas em serviços gratuitos publicados na internet (registro.br)	Baixo	É recomendado que nenhuma informação particular de funcionários ou prestadores de serviços seja exposta publicamente na internet. Verificar a possibilidade de inserir um endereço de *email* genérico com domínio corporativo, por exemplo: segurança@riocard.com
5	200.201.145.2	N/A	Disclosure of Personal Information	Informações sobre contatos e endereços de email com domínio não corporativo puderam ser identificadas através de consultas em serviços gratuitos publicados na internet (registro.br)	Baixo	É recomendado que nenhuma informação particular de funcionários ou prestadores de serviços seja exposta publicamente na internet. Verificar a possibilidade de inserir um endereço de *email* genérico com domínio corporativo, por exemplo: segurança@riocard.com
6	200.201.145.63	N/A	Disclosure of Personal Information	Informações sobre contatos e endereços de email com domínio não corporativo puderam ser identificadas através de consultas em serviços gratuitos publicados na internet (registro.br)	Baixo	É recomendado que nenhuma informação particular de funcionários ou prestadores de serviços seja exposta publicamente na internet. Verificar a possibilidade de inserir um endereço de *email* genérico com domínio

#	IP	Porta(s)	Vulnerabilidade	Descrição	Severidade	Recomendação
						corporativo, por exemplo segurança@riocard.com.

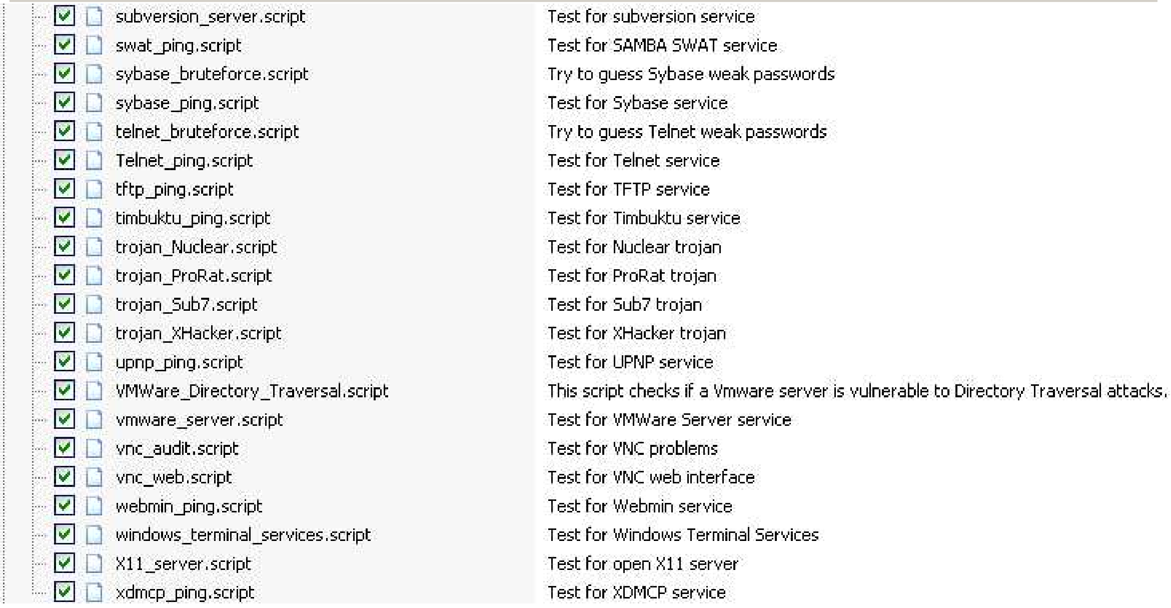
Anexo E – Lista de verificações realizadas pela ferramenta automatizada



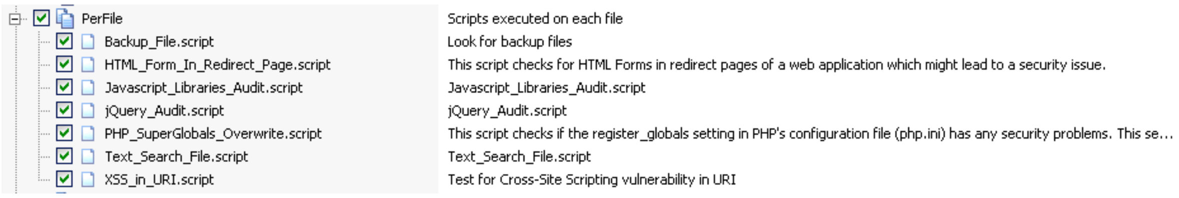
☑ Network	Network scripts
☑ chargen_ping.script	Test for chargen service
☑ crossdomain_xml.script	Test for misconfigurations in crossdomain.xml file
☑ cvs_server.script	Test for CVS server
☑ daytime_ping.script	Test for daytime service
☑ dns_cache_poisoning.script	Test for DNS cache poisoning
☑ dns_cache_snooping.script	Test for DNS cache snooping
☑ dns_open_recursion.script	Test for DNS open recursion
☑ dns_zone_transfer.script	Test is DNS zone transfer is possible
☑ dotnet.script	Test for .NET presence
☑ echo_ping.script	Test for echo service
☑ finger_ping.script	Test for finger service
☑ finger_solaris_disclosure.script	Test for Solaris finger disclosure vulnerability
☑ ftp_anonymous.script	Test for FTP anonymous login
☑ ftp_anonymous_writable.script	Test if anonymous users can create files/directories
☑ ftp_bruteforce.script	Try to guess FTP weak passwords
☑ identd_ping.script	Test for identd service
☑ imap_bruteforce.script	Try to guess IMAP weak passwords
☑ imap_server.script	Test for IMAP service
☑ ip_address_info.script	Get information about scanned IP address (WHOIS)
☑ ircd_info.script	Try to get some information from the IRC server
☑ ldap_audit.script	Test for IMAP anonymous binds
☑ lpd_ping.script	Test for LPD service
☑ mdns_zeroconf_ping.script	Test for Zeroconf service
☑ memcached_ping.script	Test for memcached service
☑ mssql_bruteforce.script	Try to guess MSSQL weak passwords
☑ mssql_ping.script	Test for MSSQL service
☑ mysqlInfo.script	Test for MySQL service
☑ mysql_bruteforce.script	Try to guess MySQL weak passwords
☑ netbios_query.script	Test if the server responds to NETBIOS queries



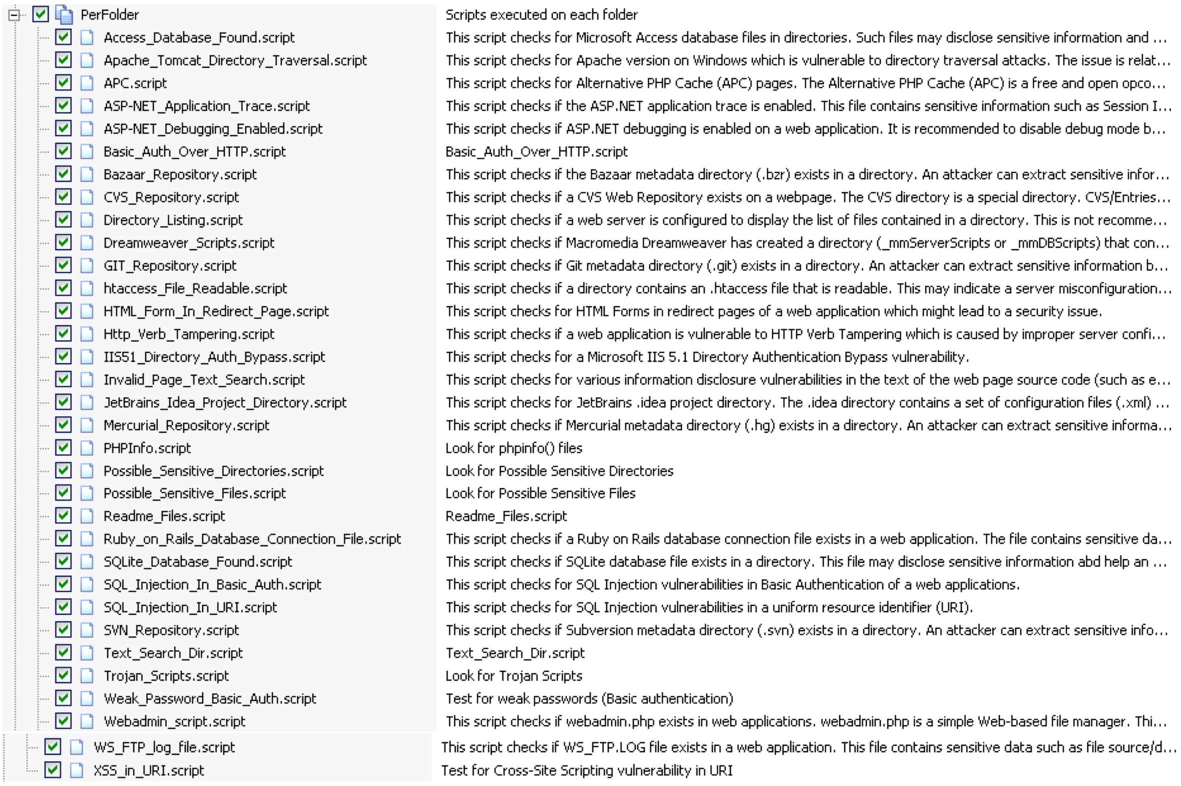
	Script	Description
☑	ntp_ping.script	Test for NTP service
☑	oracle_HTTP.script	Test for Oracle HTTP service
☑	oracle_tnssecurity.script	Test for Oracle TNS service
☑	oracle_version.script	Try to determine Oracle server version
☑	pc_anywhere.script	Test for PcAnywhere service
☑	pop3_bruteforce.script	Try to guess POP3 weak passwords
☑	pop3_server.script	Test for POP3 service
☑	Postgresql_bruteforce.script	Try to guess PostgreSql weak passwords
☑	Postgresql_ping.script	Test for PostgreSql service
☑	proxy_open.script	Test for open proxy server
☑	proxy_use_any_port.script	Test if the open proxy allows connections to any port
☑	proxy_use_connect.script	Test if the open proxy allows users to use CONNECT method
☑	proxy_use_connect_to_itself.script	Test if the open proxy allows CONNECT to itself
☑	proxy_use_post.script	Test if the open proxy allows users to use POST method
☑	rlogin_ping.script	Test for rlogin service
☑	rpc_info.script	Try to list RPC services
☑	rsh_ping.script	Test for RSH service
☑	rsync_ping.script	Test for RSync service
☑	smb_audit.script	Test for SMB service
☑	smtp_commands.script	Try to detect what SMTP commands are allowed
☑	smtp_exim_overflow.script	Test for a known Exim buffer overflow
☑	smtp_open_relay.script	Test for SMTP open relay
☑	smtp_vrfy_expn.script	Test is SMTP VRFY/EXPN commands are available
☑	snmp_ping.script	Test to guess SNMP community string
☑	socks_bruteforce.script	Try to guess SOCKS weak passwords
☑	socks_ping.script	Test for SOCKS service
☑	ssh_bruteforce.script	Try to guess SSH weak passwords
☑	ssh_ping.script	Test for SSH service
☑	ssh_random.script	Test for Debian OpenSSL predictable random number generator
☑	ssl_ping.script	Test for SSL protocol
☑	ssl_v2_hello_overflow.script	Test for SSL v2 Hello overflow



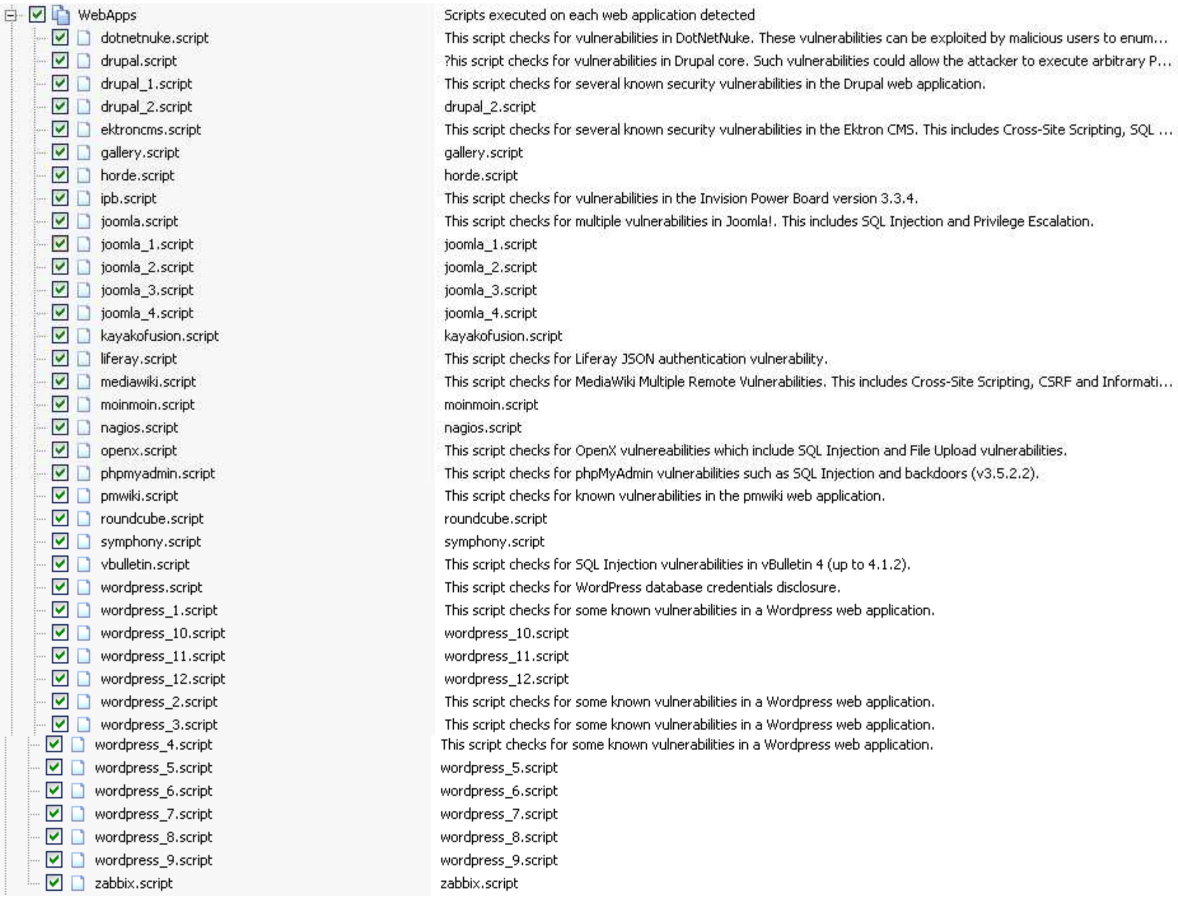
	Script	Description
☑	subversion_server.script	Test for subversion service
☑	swat_ping.script	Test for SAMBA SWAT service
☑	sybase_bruteforce.script	Try to guess Sybase weak passwords
☑	sybase_ping.script	Test for Sybase service
☑	telnet_bruteforce.script	Try to guess Telnet weak passwords
☑	Telnet_ping.script	Test for Telnet service
☑	tftp_ping.script	Test for TFTP service
☑	timbuktu_ping.script	Test for Timbuktu service
☑	trojan_Nuclear.script	Test for Nuclear trojan
☑	trojan_ProRat.script	Test for ProRat trojan
☑	trojan_Sub7.script	Test for Sub7 trojan
☑	trojan_XHacker.script	Test for XHacker trojan
☑	upnp_ping.script	Test for UPNP service
☑	VMWare_Directory_Traversal.script	This script checks if a Vmware server is vulnerable to Directory Traversal attacks.
☑	vmware_server.script	Test for VMWare Server service
☑	vnc_audit.script	Test for VNC problems
☑	vnc_web.script	Test for VNC web interface
☑	webmin_ping.script	Test for Webmin service
☑	windows_terminal_services.script	Test for Windows Terminal Services
☑	X11_server.script	Test for open X11 server
☑	xdmcp_ping.script	Test for XDMCP service



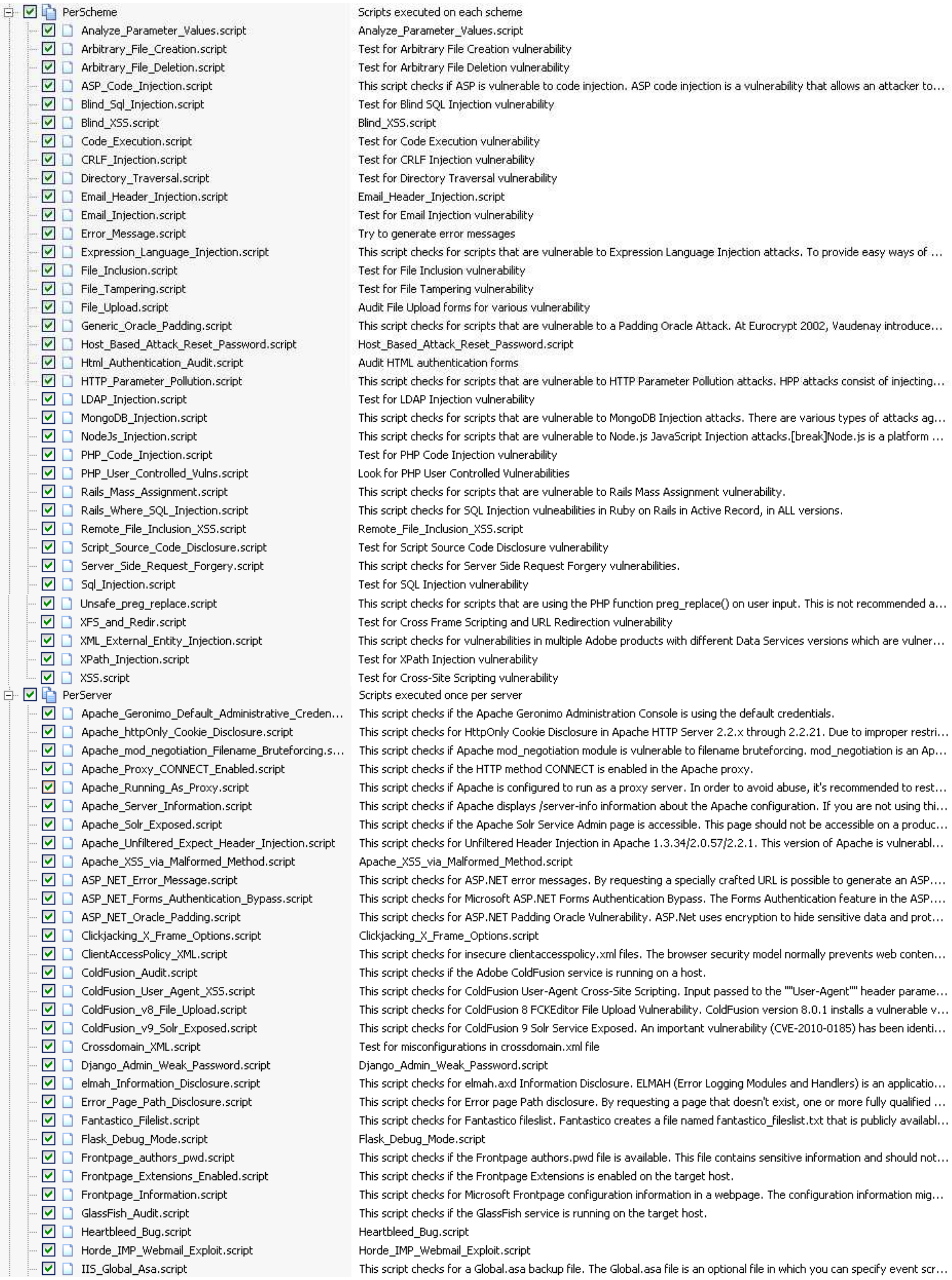
☑ PerFile	Scripts executed on each file
☑ Backup_File.script	Look for backup files
☑ HTML_Form_In_Redirect_Page.script	This script checks for HTML Forms in redirect pages of a web application which might lead to a security issue.
☑ Javascript_Libraries_Audit.script	Javascript_Libraries_Audit.script
☑ jQuery_Audit.script	jQuery_Audit.script
☑ PHP_SuperGlobals_Overwrite.script	This script checks if the register_globals setting in PHP's configuration file (php.ini) has any security problems. This se...
☑ Text_Search_File.script	Text_Search_File.script
☑ XSS_in_URI.script	Test for Cross-Site Scripting vulnerability in URI



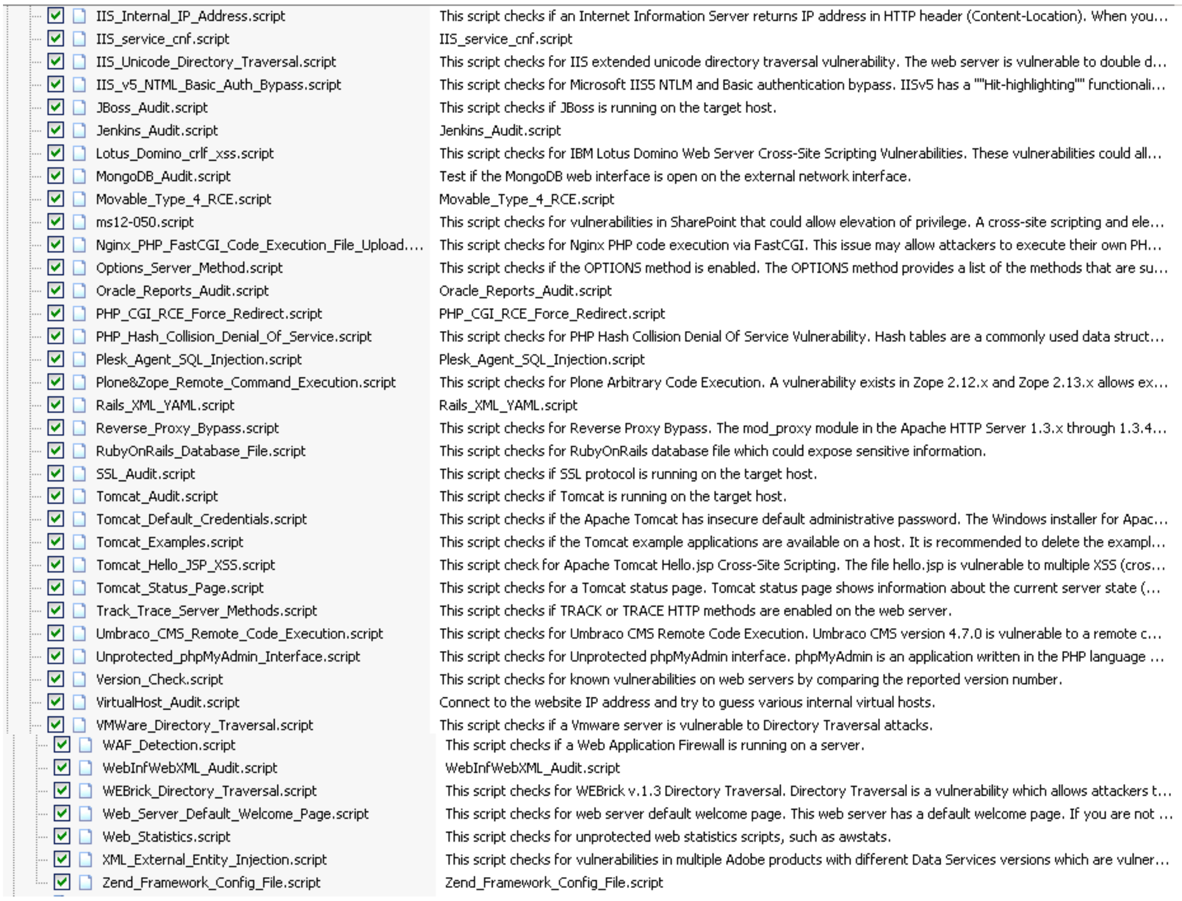
☑ PerFolder	Scripts executed on each folder
☑ Access_Database_Found.script	This script checks for Microsoft Access database files in directories. Such files may disclose sensitive information and ...
☑ Apache_Tomcat_Directory_Traversal.script	This script checks for Apache version on Windows which is vulnerable to directory traversal attacks. The issue is relat...
☑ APC.script	This script checks for Alternative PHP Cache (APC) pages. The Alternative PHP Cache (APC) is a free and open opco...
☑ ASP-NET_Application_Trace.script	This script checks if the ASP.NET application trace is enabled. This file contains sensitive information such as Session I...
☑ ASP-NET_Debugging_Enabled.script	This script checks if ASP.NET debugging is enabled on a web application. It is recommended to disable debug mode b...
☑ Basic_Auth_Over_HTTP.script	Basic_Auth_Over_HTTP.script
☑ Bazaar_Repository.script	This script checks if the Bazaar metadata directory (.bzr) exists in a directory. An attacker can extract sensitive infor...
☑ CVS_Repository.script	This script checks if a CVS Web Repository exists on a webpage. The CVS directory is a special directory. CVS/Entries...
☑ Directory_Listing.script	This script checks if a web server is configured to display the list of files contained in a directory. This is not recomme...
☑ Dreamweaver_Scripts.script	This script checks if Macromedia Dreamweaver has created a directory (_mmServerScripts or _mmDBScripts) that con...
☑ GIT_Repository.script	This script checks if Git metadata directory (.git) exists in a directory. An attacker can extract sensitive information b...
☑ htaccess_File_Readable.script	This script checks if a directory contains an .htaccess file that is readable. This may indicate a server misconfiguration...
☑ HTML_Form_In_Redirect_Page.script	This script checks for HTML Forms in redirect pages of a web application which might lead to a security issue.
☑ Http_Verb_Tampering.script	This script checks if a web application is vulnerable to HTTP Verb Tampering which is caused by improper server confi...
☑ IIS51_Directory_Auth_Bypass.script	This script checks for a Microsoft IIS 5.1 Directory Authentication Bypass vulnerability.
☑ Invalid_Page_Text_Search.script	This script checks for various information disclosure vulnerabilities in the text of the web page source code (such as e...
☑ JetBrains_Idea_Project_Directory.script	This script checks for JetBrains .idea project directory. The .idea directory contains a set of configuration files (.xml) ...
☑ Mercurial_Repository.script	This script checks if Mercurial metadata directory (.hg) exists in a directory. An attacker can extract sensitive informa...
☑ PHPInfo.script	Look for phpinfo() files
☑ Possible_Sensitive_Directories.script	Look for Possible Sensitive Directories
☑ Possible_Sensitive_Files.script	Look for Possible Sensitive Files
☑ Readme_Files.script	Readme_Files.script
☑ Ruby_on_Rails_Database_Connection_File.script	This script checks if a Ruby on Rails database connection file exists in a web application. The file contains sensitive da...
☑ SQLite_Database_Found.script	This script checks if SQLite database file exists in a directory. This file may disclose sensitive information abd help an ...
☑ SQL_Injection_In_Basic_Auth.script	This script checks for SQL Injection vulnerabilities in Basic Authentication of a web applications.
☑ SQL_Injection_In_URI.script	This script checks for SQL Injection vulnerabilities in a uniform resource identifier (URI).
☑ SVN_Repository.script	This script checks if Subversion metadata directory (.svn) exists in a directory. An attacker can extract sensitive info...
☑ Text_Search_Dir.script	Text_Search_Dir.script
☑ Trojan_Scripts.script	Look for Trojan Scripts
☑ Weak_Password_Basic_Auth.script	Test for weak passwords (Basic authentication)
☑ Webadmin_script.script	This script checks if webadmin.php exists in web applications. webadmin.php is a simple Web-based file manager. Thi...
☑ WS_FTP_log_file.script	This script checks if WS_FTP.LOG file exists in a web application. This file contains sensitive data such as file source/d...
☑ XSS_in_URI.script	Test for Cross-Site Scripting vulnerability in URI



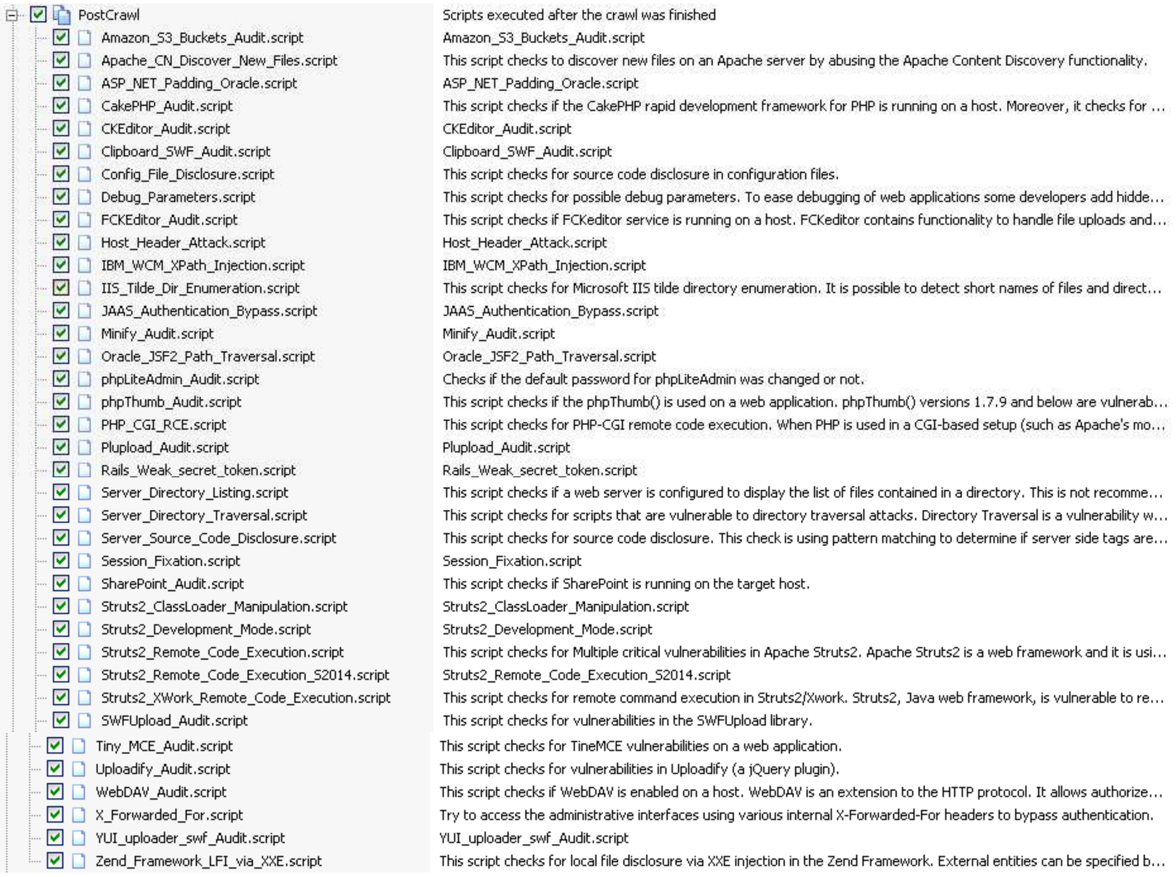
☑ WebApps	Scripts executed on each web application detected
☑ dotnetnuke.script	This script checks for vulnerabilities in DotNetNuke. These vulnerabilities can be exploited by malicious users to enum...
☑ drupal.script	?his script checks for vulnerabilities in Drupal core. Such vulnerabilities could allow the attacker to execute arbitrary P...
☑ drupal_1.script	This script checks for several known security vulnerabilities in the Drupal web application.
☑ drupal_2.script	drupal_2.script
☑ ektroncms.script	This script checks for several known security vulnerabilities in the Ektron CMS. This includes Cross-Site Scripting, SQL ...
☑ gallery.script	gallery.script
☑ horde.script	horde.script
☑ ipb.script	This script checks for vulnerabilities in the Invision Power Board version 3.3.4.
☑ joomla.script	This script checks for multiple vulnerabilities in Joomla!. This includes SQL Injection and Privilege Escalation.
☑ joomla_1.script	joomla_1.script
☑ joomla_2.script	joomla_2.script
☑ joomla_3.script	joomla_3.script
☑ joomla_4.script	joomla_4.script
☑ kayakofusion.script	kayakofusion.script
☑ liferay.script	This script checks for Liferay JSON authentication vulnerability.
☑ mediawiki.script	This script checks for MediaWiki Multiple Remote Vulnerabilities. This includes Cross-Site Scripting, CSRF and Informati...
☑ moinmoin.script	moinmoin.script
☑ nagios.script	nagios.script
☑ openx.script	This script checks for OpenX vulnereabilities which include SQL Injection and File Upload vulnerabilities.
☑ phpmyadmin.script	This script checks for phpMyAdmin vulnerabilities such as SQL Injection and backdoors (v3.5.2.2).
☑ pmwiki.script	This script checks for known vulnerabilities in the pmwiki web application.
☑ roundcube.script	roundcube.script
☑ symphony.script	symphony.script
☑ vbulletin.script	This script checks for SQL Injection vulnerabilities in vBulletin 4 (up to 4.1.2).
☑ wordpress.script	This script checks for WordPress database credentials disclosure.
☑ wordpress_1.script	This script checks for some known vulnerabilities in a Wordpress web application.
☑ wordpress_10.script	wordpress_10.script
☑ wordpress_11.script	wordpress_11.script
☑ wordpress_12.script	wordpress_12.script
☑ wordpress_2.script	This script checks for some known vulnerabilities in a Wordpress web application.
☑ wordpress_3.script	This script checks for some known vulnerabilities in a Wordpress web application.
☑ wordpress_4.script	This script checks for some known vulnerabilities in a Wordpress web application.
☑ wordpress_5.script	wordpress_5.script
☑ wordpress_6.script	wordpress_6.script
☑ wordpress_7.script	wordpress_7.script
☑ wordpress_8.script	wordpress_8.script
☑ wordpress_9.script	wordpress_9.script
☑ zabbix.script	zabbix.script



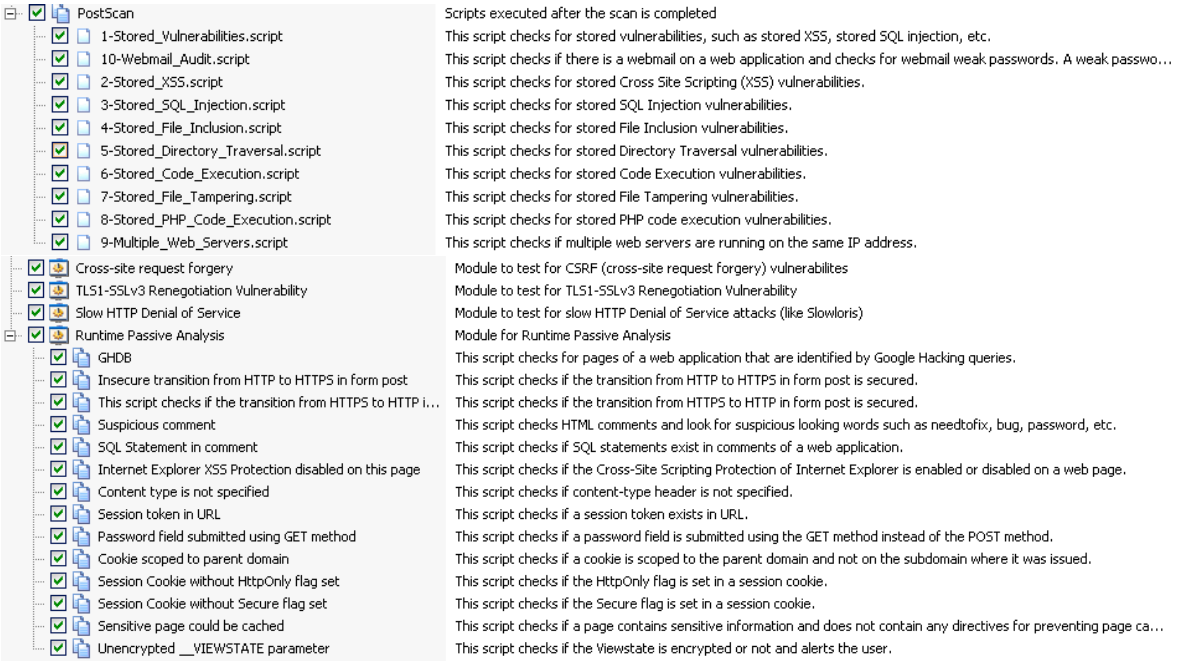
☑ PerScheme	Scripts executed on each scheme
☑ Analyze_Parameter_Values.script	Analyze_Parameter_Values.script
☑ Arbitrary_File_Creation.script	Test for Arbitrary File Creation vulnerability
☑ Arbitrary_File_Deletion.script	Test for Arbitrary File Deletion vulnerability
☑ ASP_Code_Injection.script	This script checks if ASP is vulnerable to code injection. ASP code injection is a vulnerability that allows an attacker to...
☑ Blind_Sql_Injection.script	Test for Blind SQL Injection vulnerability
☑ Blind_XSS.script	Blind_XSS.script
☑ Code_Execution.script	Test for Code Execution vulnerability
☑ CRLF_Injection.script	Test for CRLF Injection vulnerability
☑ Directory_Traversal.script	Test for Directory Traversal vulnerability
☑ Email_Header_Injection.script	Email_Header_Injection.script
☑ Email_Injection.script	Test for Email Injection vulnerability
☑ Error_Message.script	Try to generate error messages
☑ Expression_Language_Injection.script	This script checks for scripts that are vulnerable to Expression Language Injection attacks. To provide easy ways of ...
☑ File_Inclusion.script	Test for File Inclusion vulnerability
☑ File_Tampering.script	Test for File Tampering vulnerability
☑ File_Upload.script	Audit File Upload forms for various vulnerability
☑ Generic_Oracle_Padding.script	This script checks for scripts that are vulnerable to a Padding Oracle Attack. At Eurocrypt 2002, Vaudenay introduce...
☑ Host_Based_Attack_Reset_Password.script	Host_Based_Attack_Reset_Password.script
☑ Html_Authentication_Audit.script	Audit HTML authentication forms
☑ HTTP_Parameter_Pollution.script	This script checks for scripts that are vulnerable to HTTP Parameter Pollution attacks. HPP attacks consist of injecting...
☑ LDAP_Injection.script	Test for LDAP Injection vulnerability
☑ MongoDB_Injection.script	This script checks for scripts that are vulnerable to MongoDB Injection attacks. There are various types of attacks ag...
☑ NodeJs_Injection.script	This script checks for scripts that are vulnerable to Node.js JavaScript Injection attacks.[break]Node.js is a platform ...
☑ PHP_Code_Injection.script	Test for PHP Code Injection vulnerability
☑ PHP_User_Controlled_Vulns.script	Look for PHP User Controlled Vulnerabilities
☑ Rails_Mass_Assignment.script	This script checks for scripts that are vulnerable to Rails Mass Assignment vulnerability.
☑ Rails_Where_SQL_Injection.script	This script checks for SQL Injection vulneabilities in Ruby on Rails in Active Record, in ALL versions.
☑ Remote_File_Inclusion_XSS.script	Remote_File_Inclusion_XSS.script
☑ Script_Source_Code_Disclosure.script	Test for Script Source Code Disclosure vulnerability
☑ Server_Side_Request_Forgery.script	This script checks for Server Side Request Forgery vulnerabilities.
☑ Sql_Injection.script	Test for SQL Injection vulnerability
☑ Unsafe_preg_replace.script	This script checks for scripts that are using the PHP function preg_replace() on user input. This is not recommended a...
☑ XFS_and_Redir.script	Test for Cross Frame Scripting and URL Redirection vulnerability
☑ XML_External_Entity_Injection.script	This script checks for vulnerabilities in multiple Adobe products with different Data Services versions which are vulner...
☑ XPath_Injection.script	Test for XPath Injection vulnerability
☑ XSS.script	Test for Cross-Site Scripting vulnerability
☑ PerServer	Scripts executed once per server
☑ Apache_Geronimo_Default_Administrative_Creden...	This script checks if the Apache Geronimo Administration Console is using the default credentials.
☑ Apache_httpOnly_Cookie_Disclosure.script	This script checks for HttpOnly Cookie Disclosure in Apache HTTP Server 2.2.x through 2.2.21. Due to improper restri...
☑ Apache_mod_negotiation_Filename_Bruteforcing.s...	This script checks if Apache mod_negotiation module is vulnerable to filename bruteforcing. mod_negotiation is an Ap...
☑ Apache_Proxy_CONNECT_Enabled.script	This script checks if the HTTP method CONNECT is enabled in the Apache proxy.
☑ Apache_Running_As_Proxy.script	This script checks if Apache is configured to run as a proxy server. In order to avoid abuse, it's recommended to rest...
☑ Apache_Server_Information.script	This script checks if Apache displays /server-info information about the Apache configuration. If you are not using thi...
☑ Apache_Solr_Exposed.script	This script checks if the Apache Solr Service Admin page is accessible. This page should not be accessible on a produc...
☑ Apache_Unfiltered_Expect_Header_Injection.script	This script checks for Unfiltered Header Injection in Apache 1.3.34/2.0.57/2.2.1. This version of Apache is vulnerabl...
☑ Apache_XSS_via_Malformed_Method.script	Apache_XSS_via_Malformed_Method.script
☑ ASP_NET_Error_Message.script	This script checks for ASP.NET error messages. By requesting a specially crafted URL is possible to generate an ASP....
☑ ASP_NET_Forms_Authentication_Bypass.script	This script checks for Microsoft ASP.NET Forms Authentication Bypass. The Forms Authentication feature in the ASP....
☑ ASP_NET_Oracle_Padding.script	This script checks for ASP.NET Padding Oracle Vulnerability. ASP.Net uses encryption to hide sensitive data and prot...
☑ Clickjacking_X_Frame_Options.script	Clickjacking_X_Frame_Options.script
☑ ClientAccessPolicy_XML.script	This script checks for insecure clientaccesspolicy.xml files. The browser security model normally prevents web conten...
☑ ColdFusion_Audit.script	This script checks if the Adobe ColdFusion service is running on a host.
☑ ColdFusion_User_Agent_XSS.script	This script checks for ColdFusion User-Agent Cross-Site Scripting. Input passed to the ""User-Agent"" header parame...
☑ ColdFusion_v8_File_Upload.script	This script checks for ColdFusion 8 FCKEditor File Upload Vulnerability. ColdFusion version 8.0.1 installs a vulnerable v...
☑ ColdFusion_v9_Solr_Exposed.script	This script checks for ColdFusion 9 Solr Service Exposed. An important vulnerability (CVE-2010-0185) has been identi...
☑ Crossdomain_XML.script	Test for misconfigurations in crossdomain.xml file
☑ Django_Admin_Weak_Password.script	Django_Admin_Weak_Password.script
☑ elmah_Information_Disclosure.script	This script checks for elmah.axd Information Disclosure. ELMAH (Error Logging Modules and Handlers) is an applicatio...
☑ Error_Page_Path_Disclosure.script	This script checks for Error page Path disclosure. By requesting a page that doesn't exist, one or more fully qualified ...
☑ Fantastico_Filelist.script	This script checks for Fantastico fileslist. Fantastico creates a file named fantastico_fileslist.txt that is publicly availabl...
☑ Flask_Debug_Mode.script	Flask_Debug_Mode.script
☑ Frontpage_authors_pwd.script	This script checks if the Frontpage authors.pwd file is available. This file contains sensitive information and should not...
☑ Frontpage_Extensions_Enabled.script	This script checks if the Frontpage Extensions is enabled on the target host.
☑ Frontpage_Information.script	This script checks for Microsoft Frontpage configuration information in a webpage. The configuration information mig...
☑ GlassFish_Audit.script	This script checks if the GlassFish service is running on the target host.
☑ Heartbleed_Bug.script	Heartbleed_Bug.script
☑ Horde_IMP_Webmail_Exploit.script	Horde_IMP_Webmail_Exploit.script
☑ IIS_Global_Asa.script	This script checks for a Global.asa backup file. The Global.asa file is an optional file in which you can specify event scr...



☑	IIS_Internal_IP_Address.script	This script checks if an Internet Information Server returns IP address in HTTP header (Content-Location). When you…
☑	IIS_service_cnf.script	IIS_service_cnf.script
☑	IIS_Unicode_Directory_Traversal.script	This script checks for IIS extended unicode directory traversal vulnerability. The web server is vulnerable to double d…
☑	IIS_v5_NTML_Basic_Auth_Bypass.script	This script checks for Microsoft IIS5 NTLM and Basic authentication bypass. IISv5 has a ""Hit-highlighting"" functionali…
☑	JBoss_Audit.script	This script checks if JBoss is running on the target host.
☑	Jenkins_Audit.script	Jenkins_Audit.script
☑	Lotus_Domino_crlf_xss.script	This script checks for IBM Lotus Domino Web Server Cross-Site Scripting Vulnerabilities. These vulnerabilities could all…
☑	MongoDB_Audit.script	Test if the MongoDB web interface is open on the external network interface.
☑	Movable_Type_4_RCE.script	Movable_Type_4_RCE.script
☑	ms12-050.script	This script checks for vulnerabilities in SharePoint that could allow elevation of privilege. A cross-site scripting and ele…
☑	Nginx_PHP_FastCGI_Code_Execution_File_Upload.…	This script checks for Nginx PHP code execution via FastCGI. This issue may allow attackers to execute their own PH…
☑	Options_Server_Method.script	This script checks if the OPTIONS method is enabled. The OPTIONS method provides a list of the methods that are su…
☑	Oracle_Reports_Audit.script	Oracle_Reports_Audit.script
☑	PHP_CGI_RCE_Force_Redirect.script	PHP_CGI_RCE_Force_Redirect.script
☑	PHP_Hash_Collision_Denial_Of_Service.script	This script checks for PHP Hash Collision Denial Of Service Vulnerability. Hash tables are a commonly used data struct…
☑	Plesk_Agent_SQL_Injection.script	Plesk_Agent_SQL_Injection.script
☑	Plone&Zope_Remote_Command_Execution.script	This script checks for Plone Arbitrary Code Execution. A vulnerability exists in Zope 2.12.x and Zope 2.13.x allows ex…
☑	Rails_XML_YAML.script	Rails_XML_YAML.script
☑	Reverse_Proxy_Bypass.script	This script checks for Reverse Proxy Bypass. The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.4…
☑	RubyOnRails_Database_File.script	This script checks for RubyOnRails database file which could expose sensitive information.
☑	SSL_Audit.script	This script checks if SSL protocol is running on the target host.
☑	Tomcat_Audit.script	This script checks if Tomcat is running on the target host.
☑	Tomcat_Default_Credentials.script	This script checks if the Apache Tomcat has insecure default administrative password. The Windows installer for Apac…
☑	Tomcat_Examples.script	This script checks if the Tomcat example applications are available on a host. It is recommended to delete the exampl…
☑	Tomcat_Hello_JSP_XSS.script	This script check for Apache Tomcat Hello.jsp Cross-Site Scripting. The file hello.jsp is vulnerable to multiple XSS (cros…
☑	Tomcat_Status_Page.script	This script checks for a Tomcat status page. Tomcat status page shows information about the current server state (…
☑	Track_Trace_Server_Methods.script	This script checks if TRACK or TRACE HTTP methods are enabled on the web server.
☑	Umbraco_CMS_Remote_Code_Execution.script	This script checks for Umbraco CMS Remote Code Execution. Umbraco CMS version 4.7.0 is vulnerable to a remote c…
☑	Unprotected_phpMyAdmin_Interface.script	This script checks for Unprotected phpMyAdmin interface. phpMyAdmin is an application written in the PHP language …
☑	Version_Check.script	This script checks for known vulnerabilities on web servers by comparing the reported version number.
☑	VirtualHost_Audit.script	Connect to the website IP address and try to guess various internal virtual hosts.
☑	VMWare_Directory_Traversal.script	This script checks if a Vmware server is vulnerable to Directory Traversal attacks.
☑	WAF_Detection.script	This script checks if a Web Application Firewall is running on a server.
☑	WebInfWebXML_Audit.script	WebInfWebXML_Audit.script
☑	WEBrick_Directory_Traversal.script	This script checks for WEBrick v.1.3 Directory Traversal. Directory Traversal is a vulnerability which allows attackers t…
☑	Web_Server_Default_Welcome_Page.script	This script checks for web server default welcome page. This web server has a default welcome page. If you are not …
☑	Web_Statistics.script	This script checks for unprotected web statistics scripts, such as awstats.
☑	XML_External_Entity_Injection.script	This script checks for vulnerabilities in multiple Adobe products with different Data Services versions which are vulner…
☑	Zend_Framework_Config_File.script	Zend_Framework_Config_File.script



☑ PostCrawl	Scripts executed after the crawl was finished
☑ Amazon_S3_Buckets_Audit.script	Amazon_S3_Buckets_Audit.script
☑ Apache_CN_Discover_New_Files.script	This script checks to discover new files on an Apache server by abusing the Apache Content Discovery functionality.
☑ ASP_NET_Padding_Oracle.script	ASP_NET_Padding_Oracle.script
☑ CakePHP_Audit.script	This script checks if the CakePHP rapid development framework for PHP is running on a host. Moreover, it checks for ...
☑ CKEditor_Audit.script	CKEditor_Audit.script
☑ Clipboard_SWF_Audit.script	Clipboard_SWF_Audit.script
☑ Config_File_Disclosure.script	This script checks for source code disclosure in configuration files.
☑ Debug_Parameters.script	This script checks for possible debug parameters. To ease debugging of web applications some developers add hidde...
☑ FCKEditor_Audit.script	This script checks if FCKeditor service is running on a host. FCKeditor contains functionality to handle file uploads and...
☑ Host_Header_Attack.script	Host_Header_Attack.script
☑ IBM_WCM_XPath_Injection.script	IBM_WCM_XPath_Injection.script
☑ IIS_Tilde_Dir_Enumeration.script	This script checks for Microsoft IIS tilde directory enumeration. It is possible to detect short names of files and direct...
☑ JAAS_Authentication_Bypass.script	JAAS_Authentication_Bypass.script
☑ Minify_Audit.script	Minify_Audit.script
☑ Oracle_JSF2_Path_Traversal.script	Oracle_JSF2_Path_Traversal.script
☑ phpLiteAdmin_Audit.script	Checks if the default password for phpLiteAdmin was changed or not.
☑ phpThumb_Audit.script	This script checks if the phpThumb() is used on a web application. phpThumb() versions 1.7.9 and below are vulnerab...
☑ PHP_CGI_RCE.script	This script checks for PHP-CGI remote code execution. When PHP is used in a CGI-based setup (such as Apache's mo...
☑ Plupload_Audit.script	Plupload_Audit.script
☑ Rails_Weak_secret_token.script	Rails_Weak_secret_token.script
☑ Server_Directory_Listing.script	This script checks if a web server is configured to display the list of files contained in a directory. This is not recomme...
☑ Server_Directory_Traversal.script	This script checks for scripts that are vulnerable to directory traversal attacks. Directory Traversal is a vulnerability w...
☑ Server_Source_Code_Disclosure.script	This script checks for source code disclosure. This check is using pattern matching to determine if server side tags are...
☑ Session_Fixation.script	Session_Fixation.script
☑ SharePoint_Audit.script	This script checks if SharePoint is running on the target host.
☑ Struts2_ClassLoader_Manipulation.script	Struts2_ClassLoader_Manipulation.script
☑ Struts2_Development_Mode.script	Struts2_Development_Mode.script
☑ Struts2_Remote_Code_Execution.script	This script checks for Multiple critical vulnerabilities in Apache Struts2. Apache Struts2 is a web framework and it is usi...
☑ Struts2_Remote_Code_Execution_S2014.script	Struts2_Remote_Code_Execution_S2014.script
☑ Struts2_XWork_Remote_Code_Execution.script	This script checks for remote command execution in Struts2/Xwork. Struts2, Java web framework, is vulnerable to re...
☑ SWFUpload_Audit.script	This script checks for vulnerabilities in the SWFUpload library.
☑ Tiny_MCE_Audit.script	This script checks for TineMCE vulnerabilities on a web application.
☑ Uploadify_Audit.script	This script checks for vulnerabilities in Uploadify (a jQuery plugin).
☑ WebDAV_Audit.script	This script checks if WebDAV is enabled on a host. WebDAV is an extension to the HTTP protocol. It allows authorize...
☑ X_Forwarded_For.script	Try to access the administrative interfaces using various internal X-Forwarded-For headers to bypass authentication.
☑ YUI_uploader_swf_Audit.script	YUI_uploader_swf_Audit.script
☑ Zend_Framework_LFI_via_XXE.script	This script checks for local file disclosure via XXE injection in the Zend Framework. External entities can be specified b...



☑ PostScan	Scripts executed after the scan is completed
☑ 1-Stored_Vulnerabilities.script	This script checks for stored vulnerabilities, such as stored XSS, stored SQL injection, etc.
☑ 10-Webmail_Audit.script	This script checks if there is a webmail on a web application and checks for webmail weak passwords. A weak passwo...
☑ 2-Stored_XSS.script	This script checks for stored Cross Site Scripting (XSS) vulnerabilities.
☑ 3-Stored_SQL_Injection.script	This script checks for stored SQL Injection vulnerabilities.
☑ 4-Stored_File_Inclusion.script	This script checks for stored File Inclusion vulnerabilities.
☑ 5-Stored_Directory_Traversal.script	This script checks for stored Directory Traversal vulnerabilities.
☑ 6-Stored_Code_Execution.script	This script checks for stored Code Execution vulnerabilities.
☑ 7-Stored_File_Tampering.script	This script checks for stored File Tampering vulnerabilities.
☑ 8-Stored_PHP_Code_Execution.script	This script checks for stored PHP code execution vulnerabilities.
☑ 9-Multiple_Web_Servers.script	This script checks if multiple web servers are running on the same IP address.
☑ Cross-site request forgery	Module to test for CSRF (cross-site request forgery) vulnerabilites
☑ TLS1-SSLv3 Renegotiation Vulnerability	Module to test for TLS1-SSLv3 Renegotiation Vulnerability
☑ Slow HTTP Denial of Service	Module to test for slow HTTP Denial of Service attacks (like Slowloris)
☑ Runtime Passive Analysis	Module for Runtime Passive Analysis
☑ GHDB	This script checks for pages of a web application that are identified by Google Hacking queries.
☑ Insecure transition from HTTP to HTTPS in form post	This script checks if the transition from HTTP to HTTPS in form post is secured.
☑ This script checks if the transition from HTTPS to HTTP i...	This script checks if the transition from HTTPS to HTTP in form post is secured.
☑ Suspicious comment	This script checks HTML comments and look for suspicious looking words such as needtofix, bug, password, etc.
☑ SQL Statement in comment	This script checks if SQL statements exist in comments of a web application.
☑ Internet Explorer XSS Protection disabled on this page	This script checks if the Cross-Site Scripting Protection of Internet Explorer is enabled or disabled on a web page.
☑ Content type is not specified	This script checks if content-type header is not specified.
☑ Session token in URL	This script checks if a session token exists in URL.
☑ Password field submitted using GET method	This script checks if a password field is submitted using the GET method instead of the POST method.
☑ Cookie scoped to parent domain	This script checks if a cookie is scoped to the parent domain and not on the subdomain where it was issued.
☑ Session Cookie without HttpOnly flag set	This script checks if the HttpOnly flag is set in a session cookie.
☑ Session Cookie without Secure flag set	This script checks if the Secure flag is set in a session cookie.
☑ Sensitive page could be cached	This script checks if a page contains sensitive information and does not contain any directives for preventing page ca...
☑ Unencrypted __VIEWSTATE parameter	This script checks if the Viewstate is encrypted or not and alerts the user.

Anexo F - Glossário

Para garantir o correto entendimento das informações apresentadas neste relatório e evitar interpretações divergentes ocasionadas por definições diversas para um mesmo termo, apresentamos um glossário técnico que visa determinar os conceitos oficiais adotados para o projeto em questão:

Sistema de Bilhetagem Eletrônica (SBE)

Sistema por meio de cartões eletrônicos (bilhete eletrônico) pelo qual são efetuados os pagamentos no âmbito do sistema de transportes do Estado do Rio de Janeiro. É a ferramenta tecnológica gerida e operada pela RioCard, que suporta a operação do Sistema de Bilhete Único Municipal e Intermunicipal.

Usuário Cadastrado

Qualquer cidadão com situação regular no Cadastro de Pessoas Físicas (CPF) portador de um cartão eletrônico válido e que tenha preenchido o cadastro no Sistema de Bilhetagem Eletrônica.

Usuário Ativo

Usuário Cadastrado que já tenha realizado o desbloqueio do cartão eletrônico por meio da utilização do cartão eletrônico no Validador.

Validador

Aparelho instalado em cada veículo ou em estações de embarque para leitura do cartão eletrônico dos usuários e registro da transação. O Validador pode estar embarcado, ou seja, instalado em veículos dos modais Ônibus e Vans, ou fixo em terminais de embarque, no caso dos aparelhos instalados nas catracas das estações de Barcas, Metrô e Trem.

Transação

Cada registro no validador de qualquer modal que, isolada ou combinadamente com outro(s) registro(s), gerou, ao final do itinerário, algum subsídio ao usuário.

Viagem

Trajeto percorrido desde a origem até o destino. Ex.: Trajeto realizado desde o bairro de Icaraí, na cidade de Niterói até o centro da cidade do Rio de Janeiro. Este trajeto corresponde a 1 viagem.

Concessionários e Permissionários

Empresas privadas que adquiriram junto ao Estado o direito de explorar o serviço público de transporte.

Riscos

Eventos ou condições incertas relacionadas ao ambiente de TI do BUC (Bilhete Único Carioca) que, se concretizarem, poderão impactar a regra de negócio/subprocesso.

Objetivo de Controle

Procedimentos e metas necessários para mitigar os riscos mencionados.

Oportunidade de Melhoria

Percepção de uma necessidade de melhoria, para atendimento de um ponto de atenção identificado nos processos e regras de negócio avaliados.

© 2014 PRICEWATERHOUSECOOPERS CORPORATE FINANCE & RECOVERY LTDA. Todos os direitos reservados. Neste documento, "PwC" refere-se à PRICEWATERHOUSECOOPERS CORPORATE FINANCE & RECOVERY LTDA, a qual é uma firma membro do network da PricewaterhouseCoopers International Limited, sendo que cada firma membro constitui-se em uma pessoa jurídica totalmente separada e independente. O termo "PwC" refere-se à rede (network) de firmas membro da PricewaterhouseCoopers International Limited (PwCIL) ou, conforme o contexto determina, a cada uma das firmas membro participantes da rede da PwC. Cada firma membro da rede constitui uma pessoa jurídica separada e independente e que não atua como agente da PwCIL nem de qualquer outra firma membro. A PwCIL não presta serviços a clientes. A PwCIL não é responsável ou se obriga pelos atos ou omissões de qualquer de suas firmas membro, tampouco controla o julgamento profissional das referidas firmas ou pode obrigá-las de qualquer forma. Nenhuma firma membro é responsável pelos atos ou omissões de outra firma membro, nem controla o julgamento profissional de outra firma membro ou da PwCIL, nem pode obrigá-las de qualquer forma.

Obrigado!

www.pwc.com.br
&
www.strategyand.pwc.com

© 2014 PricewaterhouseCoopers Corporate Finance & Recovery Ltda. Todos os direitos reservados. Neste documento, "PwC" refere-se à PricewaterhouseCoopers Serviços Profissionais Ltda, a qual é uma firma membro do network da PricewaterhouseCoopers International Limited, sendo que cada firma membro constitui-se em uma pessoa jurídica totalmente separada e independente.

O termo "PwC" refere-se à rede (network) de firmas membro da PricewaterhouseCoopers International Limited (PwCIL) ou, conforme o contexto determina, a cada uma das firmas membro participantes da rede da PwC. Cada firma membro da rede constitui uma pessoa jurídica separada e independente e que não atua como agente da PwCIL nem de qualquer outra firma membro. A PwCIL não presta serviços a clientes. A PwCIL não é responsável ou se obriga pelos atos ou omissões de qualquer de suas firmas membro, tampouco controla o julgamento profissional das referidas firmas ou pode obrigá-las de qualquer forma. Nenhuma firma membro é responsável pelos atos ou omissões de outra firma membro, nem controla o julgamento profissional de outra firma membro ou da PwCIL, nem pode obrigá-las de qualquer forma.